GNOSIS

WHITEPAPER

22 December 2017

Contents

1. Executive Summary

Prediction markets have been poised to become one of the most disruptive innovations in capital markets and data science since the beginning of the information revolution. First proposed in the early 90s, prediction markets have yet to attract mass attention in the realm of forecasting and decision-making despite their documented efficacy for information aggregation. With the invention of powerful, peer-to-peer computing technologies such as Ethereum and Bitcoin, the scientific exploration of market-based forecasting can proceed at a rate and scale previously unimaginable. Our team believes undoubtedly that prediction markets will disrupt some of the largest existing industries in the near term. Looking forward, we expect that the Gnosis prediction market platform will form the basis for machine information economies on a global scale by realizing effective information aggregation and empowering everyone to participate.

In order for a prediction market platform to become truly disruptive, it must be universal and draw from a global liquidity pool. The platform must be decentralized, permissionless, and trustless for such a liquidity pool to exist. With these requirements in mind, the Gnosis team decided to build the platform on Ethereum.

1.1 Problem Overview

Generally speaking, the information revolution has made it easier for individuals to quickly retrieve data about any topic. However, this data often lacks context and objectivity and requires heavy lifting to produce actionable information for use in decision-making processes. The reason for this is straightforward: written information is inextricably linked to the writer's individual biases and agenda, making it difficult to delineate useful information from opinions or intentional misinformation. In other words, it's easy to find what people have said, but hard to ascertain what they actually believe.

Financial markets are particularly interesting in this regard in that the act of speculation elicits a highly effective form of information aggregation that requires no coordination (i.e. the "invisible

hand") and more closely mirrors individual beliefs. Principally, market speculators who believe they have superior information buy shares when they believe a company is undervalued and sell shares when they believe the company is overvalued. A monetary incentive exists to "update" a common data point (i.e. share price) when there is profit potential, and there is a disincentive to misreport in the form of financial loss. The resulting equilibrium share price reflects the prevailing market-wide sentiment about a company's value at any given time. In summary, information aggregation occurs with skin in the game - a characteristic that:

1. effectively glues an individual's action to their privately held beliefs and
2. is absent from other methods for information aggregation such as polling.

This is vital for understanding the principal function of prediction markets. A prediction market, in essence, aggregates information about the expected outcome of a future event[1]. Unlike a traditional financial market, prediction markets frame themselves as questions about the future. For example: Which presidential candidate Alpha or Beta will win the 2019 election? Shares are divided among predefined options (e.g. Alpha, Beta and Other) with all share values summing up to $1 (100%)[2]. Each option's share price reflects its probability of occurrence. So long as an individual believes they have superior information about the event in question, they have an incentive to purchase shares that reflect their beliefs about the outcome, thereby updating information captured by the prediction market. At the market's conclusion, the winning option's shares become redeemable for $1, while all other shares become worthless. Individual actors who purchased the winning shares receive profit equal to ($1 minus purchase price) times the number of shares held.

Over the last several decades, prediction markets have seen a surge in use due to their advantage in aggregating all available information relevant to an event's outcome. Prediction markets have already been implemented with success for a variety of applications. Initially, these markets were limited to academic purposes, the first of which being the Foresight Exchange. Perhaps Intrade was the most straightforward and general of early commercial efforts. Their platform hosted prediction markets on decidable events such as elections, current events, and epidemics. During its existence, Intrade showed that such markets could garner significant volume and estimate the likelihood of potential outcomes with greater accuracy than traditional polling methods. Also, several academic studies have shown that prediction markets are not only useful for tracking and forecasting emerging epidemics, but are in fact much more efficient and faster in doing so than other existing surveillance systems[3]. Prediction markets aggregate expert opinion quickly, accurately, and inexpensively, which is of tremendous effect in the prevention of epidemics where timely information allows for planning and allocation of resources to help with treatment and preventative interventions. More recently, prediction markets' potential has been more widely recognized and they have found use as internal tools to inform organizations, such as large corporations and nonprofits.

However, prediction markets can only rise to their full potential when tapping into a global liquidity pool for information. For this to happen, a platform needs to be truly impartial with hardwired rules for all to see. Where this is not the case large corporations with enough clout and a large enough user

[1] Prediction markets are also known as predictive markets, information markets, decision markets, idea futures, event derivatives, or virtual markets.

[2] USD 1 is the standard value set in our platform for each set of outcome tokens.

[3] International Journal of Medical Informatics: "The wisdom of crowds in action: Forecasting epidemic diseases with a web-based prediction market system", 2016: 35-43 and Healthcare Epidemology: "Use of Prediction Markets to Forecast Infectious Disease Activity", 2007: 44.

base create monopolies or at best oligopolies – in effect stopping smaller players from participating. This results in the oligopolies we see in so many areas of technology: There are a small number of ride-sharing apps, a small number of search providers, a small number of navigation apps. These oligopolies make the cost of creating a marginal benefit enormous. Let's give an example: Someone may be able to raise the quality of routing in a navigation app within a single neighborhood by contributing detailed knowledge on how the traffic lights are programmed or at which times the train crossing results in an additional few minute delay on some route or other. While this is useful information, it is not economically viable for the person or company who holds this knowledge to create a new navigation app from scratch. If they can instead contribute this knowledge to an open and impartial platform with transparent rules that cannot simply be changed by a single other player, the entire game changes: Suddenly previously siloed information becomes available for all to benefit from. Having this true impartiality that is needed for a viable prediction market platform to thrive is made possible by blockchain technology.

1.2 Mission Statement

> "Our mission is to build a truly impartial exchange for information aggregation to quantify the future. A permissionless and decentralized platform built on Ethereum, Gnosis is the easiest way to aggregate relevant information from both human and AI agents into one number."

It often is after-the-fact that we realize how much harm results from a decision made by key players such as governments, firms, or organizations. Before such a decision was made, there were certainly people who had a deep understanding about its consequences and therefore good reasons to disapprove it. However, these relevant experts were not enticed enough to share their knowledge with properly-motivated decision makers, nor were non-experts induced to learn that these decisions are inferior. Most importantly, decision-makers ultimately are not held accountable if the decision turns out to not have the consequences they promised.

An important contribution to the implementation of inefficient decisions is that our *information institutions*, i.e. public relations teams, organized interest groups, news media, discussion forums, think tanks, universities, journals, elite committees, and state agencies, fail to induce people to acquire and share relevant information. As the economist Hayek describes, markets make us not only acquire, but also convey knowledge and beliefs. Their inherent dissemination of information through market prices best reflects the dispersed knowledge which all the different individuals possess[4]. Since markets excel at encouraging people to acquire information, share it via trades, and aggregate that information into consensus prices that convince wider audiences, they seem to be ideal information institutions.

We plan to offer information markets with open, equitable, and transparent access. Gnosis operates as an open platform where access is unbiased and transparent, it can be reached from anywhere

[4] *"Competition is essentially a process of the formation of opinion: by spreading information, it creates that unity and coherence of the economic system which we presuppose when we think of it as one market. It creates the views people have about what is best and cheapest, and it is because of it that people know at least as much about possibilities and opportunities as they in fact do. It is thus a process which involved a continuous change in the data and whose significance must therefore be completely missed by any theory which treat these data as constant."* In Hayek, F.A., 1946. The Meaning of Competition. Reprinted in Hayek, F. A., 1948. Individualism and Economic Order.

and provides the same markets, pricing, and liquidity to all parties. Anyone with internet access can ask a question and fund a prediction market to find the answer, and anyone can predict an event along with billions of other market participants from all across the globe. Our exchange for information provides everyone with the same opportunities, and hence produces the most reliable forecasts.

With Gnosis, we hope to drive change in a number of important global markets, including finance, insurance, and information. Gnosis prediction markets can also be used for new forms of distributed, market-based governance protocols, and will provide unique incentivization opportunities for both local and global economies.

Gnosis also is well-positioned to help facilitate a long-term shift toward information arbitrage economies that will power the Internet of Things (IoT), as well as more advanced forms of artificial intelligence. We believe that machine intelligence will leverage a global liquidity pool of information for decision-making and will be deeply interwoven on the shared blockchain fabric of Ethereum. Decentralized prediction markets seeded on Gnosis will be the ideal medium of exchange for these intelligent agents.

1.3 Core Objectives

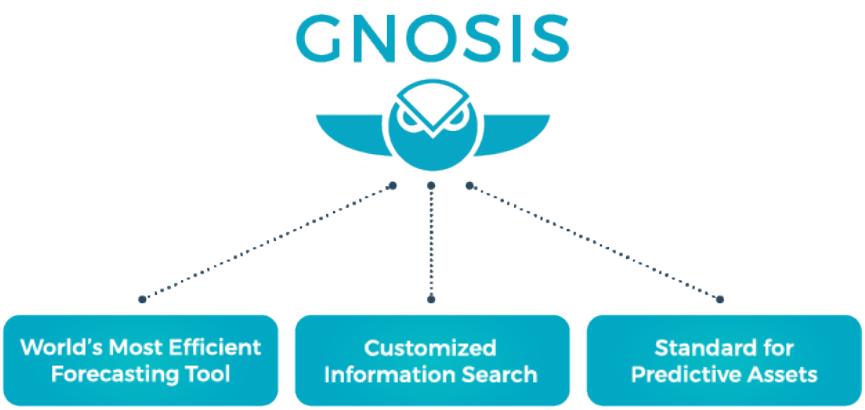

Figure 1.1: Gnosis Core Objectives

We believe that prediction markets will enable a more efficient and informed world. Rather than setting up a polling panel with a predefined group of experts who are thought to possess useful information based on criteria used by the person who makes the selection, prediction markets create an incentive for individuals with relevant information to come forward and trade that information, thereby revealing it to the market. Individuals without the relevant information are incentivized to acquire it in order to participate in the market and gain profits.

As a permissionless and decentralized platform built on Ethereum, we equally enable everyone to participate in a market. This democratization of access provides the foundation for efficient information aggregation. Prediction markets and oracles will bridge real world events to the blockchain, thereby leveraging its value as an authoritative source of truth about the world. We aim to provide the **World's Most Efficient Forecasting Tool**.

Gnosis enables anyone to ask a question and fund the search for answers. Empowering everyone to participate in the aggregation and efficient evaluation of information, this creates new economic opportunities for subject matter experts and more efficient avenues for crowdsourcing. The power of "search" is decentralized and inclusive. It will ultimately become the "Google" of **Customized Information Searching**.

Gnosis seeks to establish a global, open prediction market platform with a single liquidity pool. This resource enables the simple creation of custom prediction market applications and embodies a flexible marketplace for blockchain oracle services. We strive to set a **Standard for Predictive Assets**, creating a norm for information exchange. The information represented in a specific asset will be structured in a way that enables automated information trading, not only between humans but also between AIs, sensors, bots, and companies. This will enable automated smart decision making ranging from electricity usage when it's the cheapest to direct response of supply chains for predicted or increased demand.

2. Roadmap

2.1 Current State

Gnosis has been under development for almost three years starting at the beginning of January 2015. Since then, there were multiple iterations on different levels including changes in the Gnosis core, release of the first products and a developer tool.

In addition to developing Gnosis' core infrastructure, Gnosis has been developing other products like the Gnosis multisig wallet (*https://wallet.gnosis.pm*) which is used by several projects (e.g.: Golem, Aragon, Civic, and district0x) and sets an industry standard for secure fund management. Currently we are improving the user interface for our multisig wallet aiming to create a more user-friendly version in both enterprise and personal edition supporting two and more factor authentication on mobile devices and ledgers.

We launched Gnosis Olympia, a test version of our prediction market platform allowing participants to try out trading in prediction markets. Our management interface, the actual prediction market platform for users to trade in prediction markets is live on the mainnet since the end of 2017. Users are able to buy and sell shares in markets, and navigate to their current holdings. With its intuitive and clean UX/UI, the management interface is a first step towards user-friendly dApps and sets the standard for future dApp development in the ecosystem.

Another project we have been devoted to in 2017 is the implementation of a decentralized exchange for ERC-20 tokens based on the Dutch auction principle. We strongly believe that adapting this mechanism will lead to fair market prices. We hope to go live in early 2018.

We are eagerly working on making it as easy as possible for developers to build their own prediction market use cases with Gnosis. Our first developer tool was successfully adopted during the hackathons we participated in in 2017. We will continue improving the DevKit by incorporating the developer feedback. We aim to provide an environment in which developers can easily setup and access everything needed to start coding on our platform. Along with the new DevKit, we will introduce several developer incentivization programs beginning of 2018.

In April 2017, we had our token sale based on a modified dutch auction and successfully raised Ether worth $12.5 M. We used the funding to further expand Gnosis. The Gnosis team grew steeply in

2017 and consists today of 34 employees around the world and counting. A majority of the GNO tokens that are held by Gnosis will be used to incentivize projects and developers building on top of Gnosis. We are introducing two developer incentivization programs to support the community creating and promoting decentralized prediction markets on Gnosis[1].

2.2 Roadmap

Figure 2.1: Roadmap 2018

[1]For more information please refer to 6.2.2 Gnosis X and chapter 6.2.3 Gnosis Y.

3. Platform Model

3.1 Gnosis Layers

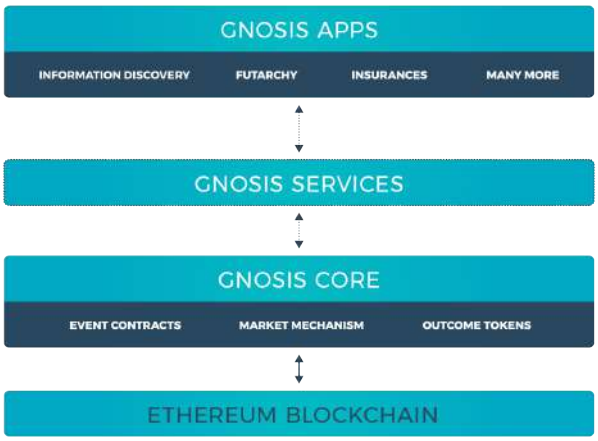

Figure 3.1: Primary layers of the Gnosis platform

Gnosis Core layer provides the foundational smart contracts for Gnosis use: event contracts that are governing the outcome token creation and settlement, and a market mechanism. This layer is and always will be free and open to use. The only process that incurs fees is the outcome token creation, which has a maximum fee of 0.5 percent, and affects traders buying outcome tokens from the market maker. This fee may be reduced by Gnosis in time. Creating new markets carries gas costs only. 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.

The **Gnosis Service layer** will offer additional services on top of Gnosis Core and will use a trading fee model. These services will comprise optimization tools like chatbots and stable coins. More features may be introduced as deemed useful. These components are necessary for most consumer applications building on Gnosis. While some applications and participants will interact with Gnosis on the Core level, we are confident that these services will be used widely.

On top of the Services layer (or in some cases, just Gnosis Core) is the **Gnosis Applications 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. As we'll see in the next section on tokens, many Gnosis applications may include token holding as a core component of their business model.

3.2 Our Token Model

The tokens that were sold during the Gnosis token sale on April 24th, 2017 are known as Gnosis tokens, or GNO. This was the only time that GNO tokens were created, and the total supply of GNO is fixed to 10 million GNO which are tradable on several exchanges.

Fees will be charged to participants for using Gnosis as a platform every time new outcome tokens are created. ERC20 compatible outcome tokens are created for every event outcome. That means that every event contract will be associated with at least two outcome tokens (for a prediction market asking "Where will Amazon locate its next headquarters?", the outcome tokens would be a) Phoenix, b) Chicago, c) Austin, or d) other).
These platform fees can be paid in OWL tokens. One OWL can be used to pay for the equivalent of one USD in fees. While paying fees in OWL is the expected and preferred form to pay fees, alternatively, fees can also be paid with the token a prediction market is traded in. This ensures efficient markets even under a temporary shortage of OWL tokens. In addition to paying fees in OWL, some prediction markets may be even traded in OWL. In this case, predictions and initial funding can be made with OWL.

3.2.1 GNO generate OWL

Gnosis tokens (GNO) are the generators for OWL tokens. OWL can only be created via activating the utility of the GNO tokens. This is done via a smart contract system. The smart contract works as follows: A GNO token holder "locks" a number of their tokens in a smart contract. Locked GNO tokens cannot be traded or transferred. The holder can specify the lock period. The amount of OWL tokens that are then created depends on the length of the lock period and the total amount of OWL tokens in the market.The total amount of OWL to be in circulation is targeted to be 20 times the average monthly usage of OWL for the preceding 3 months.

The smart contract applies the selected lock duration to a formula that is designed to regulate the total market supply of OWL tokens. Prior to locking their GNO tokens in the smart contract, users will be able to see exactly how many OWL they will receive as a result of executing the locking transaction. Once users lock their GNO, 30% of the total OWL they will get from locking their GNO

will be distributed for immediate use, and the remaining 70% will be distributed proportionally over the lock duration. Once the lock expires, the locked GNO cease to generate OWL and the GNO can be transferred again. There is no limit (other than duration) for how many times GNO tokens may be used to create OWL. There is also no limit amount of GNO tokens that can be locked.

OWL used to pay for fees are not credited to Gnosis or any other market participants but are instead consumed ("burned"). If the event's collateral token (the currency in which the event is traded in) is used to pay the fee, this token will be converted into GNO by the Gnosis smart contract system using an auction mechanism. These GNO tokens will then be used for fee reduction mechanisms and permanently held by the fee reduction contract. Burning OWL or GNO means that they will be collected in a smart contract that cannot be accessed by anyone.

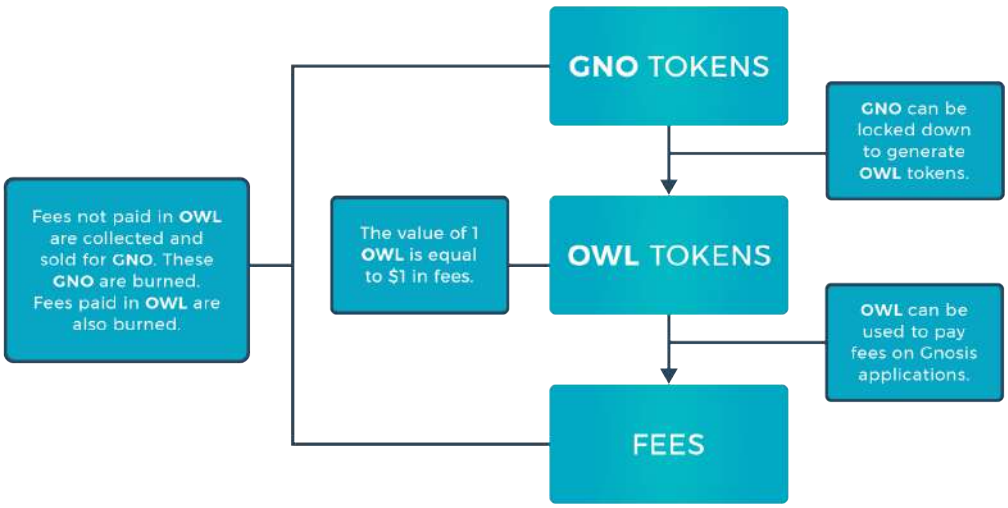

Figure 3.2: Token Machanism

3.2.2 Why would users pay in OWL when they can also use other ERC20 tokens?

A core value proposition of Gnosis (and decentralization) is to guarantee future characteristics of platforms to both users and developers without relying on the trustworthiness of an operating company. In order to do this, elements, including fee rates, must be codified into the software itself. It is expected that OWL will be the overwhelmingly predominant method for paying fees in the Gnosis ecosystem due to the following reasons:

1. It is utility that arises from locked GNO tokens
2. When OWL is used, holding GNO will generate new OWL
3. There will likely be an inflationary mechanism built into it where more OWL tokens are created if less than 90% of the fees are paid with OWL

4. Gnosis Products

4.1 Management Interface

The Gnosis Management Interface allows users to trade in prediction markets: From the main dashboard of the Management Interface, users deposit and withdraw funds. The dashboard gives an overview of the ERC-20 token balance the user is currently holding, predicted profits from the user's investments as well as the number of markets s/he has participated in. A summary of the user's token holdings and trades from the markets s/he participated in will show up in the bottom section. A dedicated markets page provides the user with an overview of all prediction markets, indicating the amount of available markets, markets resolving soon (within the next 72h), and recently created markets (created in the last 72h). From the sidebar, this view can easily be filtered by already resolved markets, markets the user has traded in, or markets which are closing soon.
From within a market's detail page, users are able to buy or sell shares in a market and navigate to their current holdings. The user can trade in categorical or scalar markets. For example, a market for a categorical event could ask *"Where will Amazon locate its next headquarters?"* with the outcomes of a) Phoenix, b) Chicago, or c) Austin. An example for a scalar market could be *"What will Apple's Stock price be at the end of Q4 2017"*. The outcome must be a scalar value—in this case a price in USD. Scalar events are represented with two outcome tokens. One outcome token for long positions [*"the price will rise"*], and one for short positions[*"the price will fall"*].
The market detail page displays more detailed information about the market such as creator of the market, Oracle and token type, fee percentage, total funding, or current number of earnings in the sidebar. A chart of the different outcome tokens (for categorical events) or short/long tokens (for scalar events) over a time period of a month, a week, or a day will be displayed in the bottom section. With its intuitive and clean UX/UI, the management interface is a first step towards user-friendly prediction market dApps and sets the standard for future dApp development in the ecosystem.

4.2 Multi Signature Wallet/Gnosis Safe

By requiring multiple users to approve a transaction, multisignature wallets enable groups of people to collectively control their funds. The Gnosis Multisig wallet sets a standard to secure fund

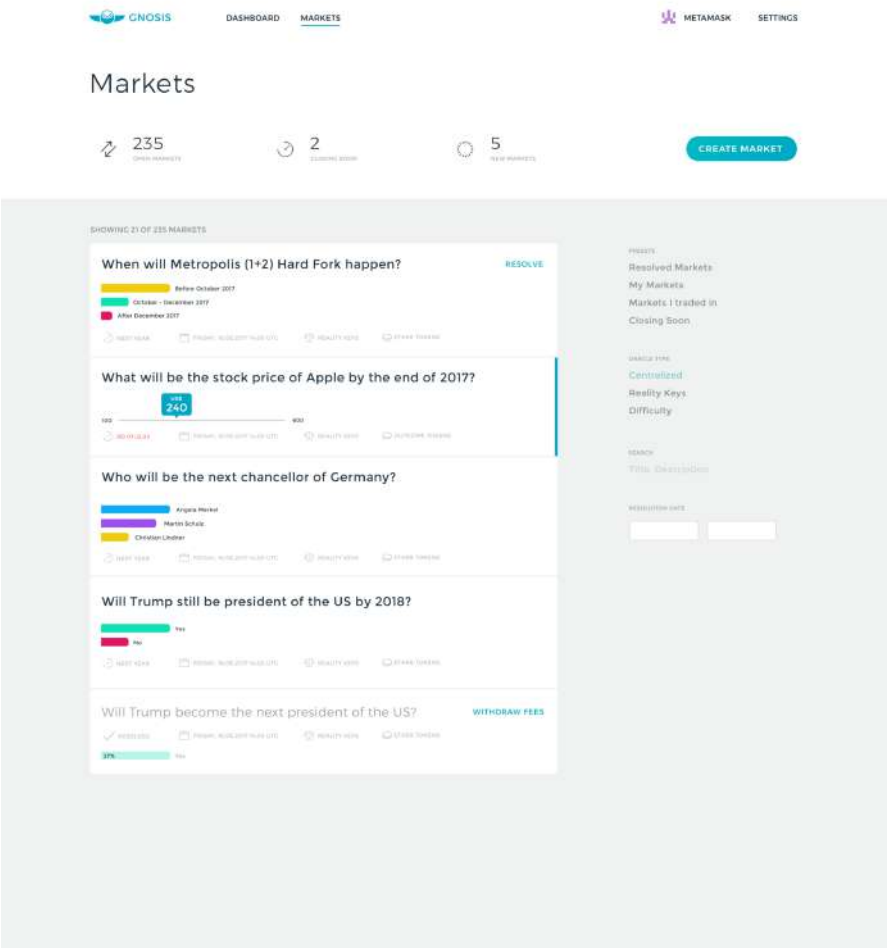

Figure 4.1: Screenshot Management Interface

management: It holds Ether and other ERC-20 tokens, integrates with web3 wallets (e.g. Metamask), supports offline signing, hardware ledgers, and allows users to configure both owners and number of required signatures. In Q1 2018, we will launch a new multisig wallet - the *Gnosis Safe*. It will offer similar functionality as the Gnosis Multisig, but is geared towards single users using two or more factor authentication. The additional factors can be held by mobile devices (phones, tablets) and hardware ledgers. Gnosis Safe will be available for mobile clients (Android, iOS) and as a Chrome extension.

4.3 Dutch Exchange

The current implementation of order book based centralized and decentralized exchanges faces some major shortcomings: The high risk of fund loss, difficulties for less liquid markets, and practices like front-running. To remedy these drawbacks, Gnosis is developing the Dutch Exchange - a decentralized exchange for ERC-20 tokens based on the Dutch auction principle. The exchange switches between two states: the state before an auction has started (for sellers to deposit their tokens), and the state of a running auction (when buyers are active). Sellers can submit the tokens

they would like to sell at any point in time. Those will automatically be placed into the next available auction - no tokens can be submitted into the running auction.

There are no fixed start times for an auction. While the final mechanism hasn't been decided upon yet, an auction will likely start at the earliest 10 minutes after the last auction for a particular token-pairing (GNO/ETH e.g.,) closed, and it only starts if sellers deposited at least an equivalent to 1,000 USD worth of tokens in the auction.

When an auction for a token-pairing starts, the initial price is set at twice the final closing price of the previous auction (of the same pairing). From this initial price, the price falls according to a decreasing function. During this state, buyers are active: buyers submit their bid at the point in time where the current price reflects their maximum willingness to pay, and they can only submit their bids until the auction closes.

An auction closes when the price clears the quantity of tokens sold and bought. Every buyer receives their tokens at the closing time for the same price. Since buyers will only pay the final market clearing price, which is either at their bid or lower, they have an economic incentive to submit the bid at their highest willingness to pay.

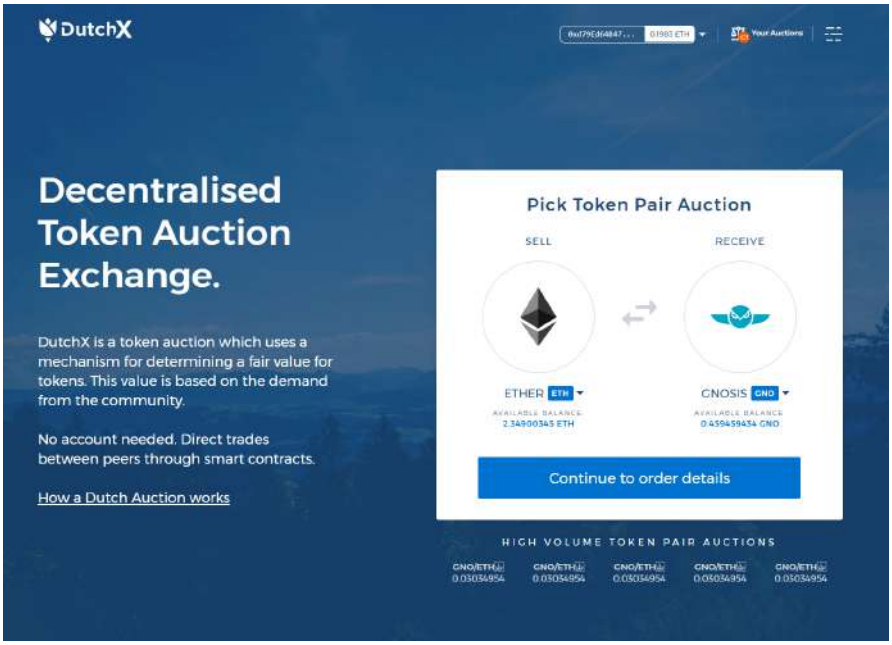

Figure 4.2: Screenshot DutchExchange

Together with the individual bid a successful buyer has made, the final price determines the amount of tokens to be received, which is at least the amount indicated at the bidding time. Buyers can request a partial payout at any time, which can be triggered an unlimited number of times. If triggered for the first time, this number is the minimum possible payout that the buyer would receive at that moment in time. If triggered any time after the first payout, the buyer will be issued the difference between the already received payout and the amount of tokens s/he would receive at the current price point.

This is also true for the time the auction closes.

One drawback of the auction model is that the exchange is not instantaneous (and funds can't immediately be withdrawn), which makes fast trading impossible. However, this is secondary to achieving a fair price.

5. Ongoing Research

5.1 Futarchy – Experiment to safeguard against malicious attacks'

Thanks to a generous grant from the Ethereum Foundation, Gnosis will be running a series of experiments to test the viability of Futarchy. Over the next two months we will be running experiments that will experimentally verify whether futarchies are manipulation resistant even if special bribes are paid to a potential attacker.

In each of these experiments, we are simulating a decision process, as for example the decision for a better CEO for a company. We assume that there is common knowledge that one of the two conditional markets will perform better than the other. In order to have a non-manipulable source of randomness, we will use the block difficulty as a metric simulating a performance metric in the Futarchy. This means that we will have two conditional markets predicting a scalar: One market - representing the company performance of a CEO A - will predict the Ethereum difficulty and the other market - representing the company performance of a CEO B - will predict the Ethereum difficulty times 1.05.
If an attacker is able to manipulate the market predicting the difficulty to surpass the price for the market predicting the difficulty times 1.05, this corresponds to the Futarchy being manipulated successfully and the wrong CEO consequently being chosen. In the experiments, we will systematically vary the bribe, the decision functions of a Futarchy, the bribe payout function and test the impact of all of these variations on the behavior of manipulators and honest traders.

Through these experiments and general tools which we plan to create on Gnosis, we aim to forge a solid platform for DAOs (and other types of organizations) to use Futarchy to inform and automate their decision making.

A further theoretical and empirical research subject will be "tokenized futarchies". Tokenized futarchies utilize tokens as collateral in the prediction markets, whose inherent value also depends on the prediction metric. There are good reasons to believe that these tokenized futarchies can be set

up in an even more manipulation-resistant manner. We want to explore these potential setups.

5.2 Distributed Key Generation

We will also be investigating distributed key generation (DKG) as a means of blinding exchange transactions sent to the blockchain. DKG enables a party to collectively generate a cryptographic key pair which can be used for public key operations such as asymmetric encryption. The decryption of ciphertexts encrypted with the party key then requires the coordination of a threshold of the key generating party.

This technology may help free decentralized order book cryptocurrency exchanges from centralized control and market manipulation tactics such as miner front-running by allowing orders to be encrypted without a single party being able to decrypt the order. It can also support other distributed protocols and enrich the crypto space in general. We are building a distributed key generation implementation based on the elliptic curve discrete log problem[1]. We will also collaborate with other major players in the space such as Parity[2] in order to ensure that DKG becomes a useful and open piece of technology for the decentralized web.

5.3 Frequent Batch Auction Exchanges

Exchanges which operate on a mechanism in which orders are collected into batches and uniformly cleared on a regular basis are called frequent batch auction exchanges. In traditional finance, this type of exchange was proposed in order to counter high frequency trading front-running tactics for rent extraction. In the blockchain space, this can help prevent similar miner front-running tactics.

We will research possible implementations of frequent batch auction exchanges. The implementations will focus on scalable, censorship-resistant and decentralized exchanges, and include the aforementioned Dutch auction based model. This exchange will act as a price-feed oracle, helping inform token mechanisms such as the OWL issuance formula.

[1] Tang, Caimu. *ECDKG: A Distributed Key Generation Protocol Based on Elliptic Curve Discrete Logarithm.*
[2] Parity. *"Secret Store." GitHub*, github.com/paritytech/parity/wiki/Secret-Store.

6. Building on Gnosis

6.1 Some Examples of Use Cases

With the Gnosis prediction market platform serving as a global liquidity hub, decentralized application developers will be able to create new classes of predictive assets that can be used in any number of simple or complex applications. The following section will introduce a set of innovations that are readily implementable in existing markets with the use of Gnosis prediction markets. It will also attempt to define entirely new verticals that are made possible through the use of predictive assets.

The Gnosis team and our advisors are resolutely pursuing strategies to bring the benefits of Gnosis and the information sharing economy to the globe as quickly as possible. We are closely working with well-established law firms in various jurisdictions and seeking legal clarity regarding the required approvals. DApps built on Gnosis might, however, be regulated in some jurisdictions. Anyone building on top of Gnosis is responsible for getting informed about the regulations concerning their products and for acquiring any required licences.

6.1.1 Information Gathering

Prediction market applications for information sales can be broken into two major categories: sales of superior information (e.g. from experts), and sales of device data. The purchase of superior information (e.g. from experts) has an incredibly high utility. For example, a market could be created asking, "What is this painting worth?" Gauging the price of a piece of art before the auction is vital for auction houses. These houses can save millions of dollars with prediction market insights into variables such as where to begin auction pricing, and how much profit to guarantee to sellers. Prediction markets can garner the expertise of specialists.
The latter category of device data sales may result in more efficient IoT optimizations, but it requires prediction market scaling tools (e.g. state channels[1]) to achieve high frequency participation with

[1] State Channels is a design pattern for scalable decentralized apps which works by moving the bulk of transactions offchain, so they resolve instantly, cost no gas, and can be private (https://media.consensys.net/state-channels-ethereum-is-open-for-business-5b7cd4d7506c).

low transaction cost. An example of this application could be smart cars participating in a market asking, "What is the traffic speed at this location?". Such a market resembles something like Waze, a consumer GPS navigation application, but for machine-to-machine interactions, providing a profit opportunity for sensor devices reporting probability estimates used to directly optimize IoT operations. In this case the markets on traffic speed could be used for driverless car routing or map services.

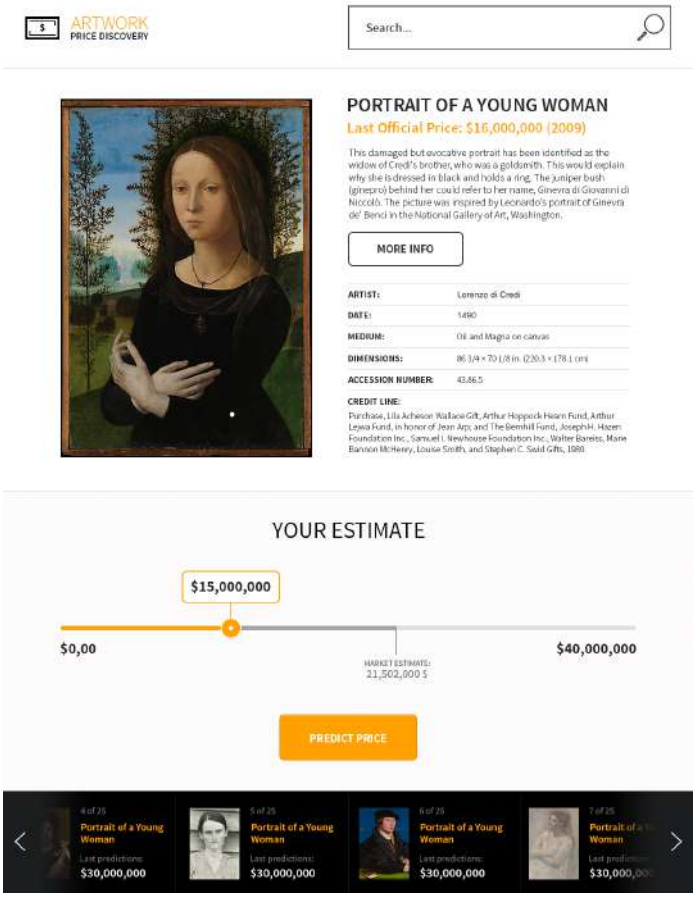

Figure 6.1: Information gathering: Gauging the price of a piece of art before the auction.

6.1.2 Incentivization

Apart from estimating event probabilities, prediction markets can be used to incentivize actions in the real world. An agent wishing to incentivize an action creates a market asking "Has a particular event occurred?" or "Will this event occur at a particular date?" Following the creation of these markets, the creator aggressively buys shares in the "No" outcome. Assume a participant observes the prediction market and believes s/he can implement the action described. By buying "Yes" shares at low cost in the market, this participant is effectively guaranteeing payment if they can complete the action, resolving the market in their favor.

An example of this applied mechanism is a market for zero-day software security exploits. In this case, a company could ask, "Will a zero-day exploit be discovered in our software?" A penetration

tester would attempt to discover exploits in the software. If an exploit is found, the tester would buy shares in the market for "Yes, an exploit will be discovered," and then reveal the exploit, either directly to the company by openly releasing the exploit or by using it in practice. For this particular application, the company would likely benefit from creating a secondary smart contract which pays the tester an additional amount for revealing the exploit privately to them.
There are many other positive use cases of the incentivization mechanism which is why we find it particularly interesting. Markets can be designed to impact a particular outcome such as the limitation of carbon dioxide emissions or the construction of new hospitals or other infrastructure projects, making the platform also an efficient tool for development cooperation.

6.1.3 Futarchy

Decision making is at the core of all governance models. Organizations must make decisions on which policies to implement in order to maximize future welfare. For a government, this could mean deciding how to budget annual tax revenues among competing policy initiatives. Take, for example, the following questions:

> "Should a portion of the budget be allocated for infrastructure projects or for digitalization? Which option will result in greater GDP?"

Within a corporation, many decisions must be made over the course of a fiscal year, with variations in frequency, time sensitivity, and value to the firm. Disputes can arise within a broad class of decisions at all levels of a company, many of which can be catastrophic if poorly executed.
In most cases of governance, such decisions are made using a hybrid of democratic and autocratic processes. The former involves a voting process in which members of an organization or government cast votes (allocated through an egalitarian or proportional representation) where a plurality, majority, or supermajority is required to implement a decision. The latter involves a hierarchical model in which designated individuals make absolute decisions over their domains of control. Metrics on share price or future revenue may be the deciding factors for evaluating the resulting performance at a later date. Both of these models suffer from information and coordination inefficiencies, often resulting in the implementation of policies and actions that poorly optimize organizational welfare.

Futarchy, coined by Robin Hanson of George Mason University, offers an alternative, market-based approach to governance. In Futarchy, markets are used to decide on and implement policies. These markets follow a general form of:
"What will a future welfare metric be if a policy is implemented?" For example, a corporation could ask, "What will our Q4 revenue be if we fire our CEO?" (Market A) and conversely, "What will our Q4 revenue be if we don't fire our CEO?" (Market B). We can refer to these bi-directional markets as decision markets. Speculators who believe they hold unique insights into the outcome of firing or keeping the CEO are incentivized to participate in both markets. If the speculator believes that revenue will be maximized by firing the CEO, then s/he will buy long shares in the company's expected revenue $[E(r)]$ if the CEO is fired and short shares in the E(r) if the CEO is not fired. Upon market closure, a decision is made corresponding to the greater expected outcome. In our CEO example, if the market value for Market A E(r) is greater than Market B E(r), then the organization fires the CEO. Market participants are then rewarded depending on their accuracy in predicting future revenue.

In this model, governance is both marketized and automated. Policies are determined by values found on an open market and implemented either through bonded delegates or an automated

process. Prediction markets have shown to be the most efficient information aggregation tool, lending credence to the hypothesis that Futarchy can more accurately identify policies that will optimize outcomes while also lowering bureaucratic overhead.

6.1.4 Financial Instruments

Prediction markets can enable the creation of financial instruments that track stock price or commodity value with greater specificity than existing derivatives. If we conceptualize traditional financial instruments as expressions of economic value, one could argue that the "expressiveness" of current market offerings is limited to statements of ownership in an asset (e.g. currencies, equities), of financial relationships between economic entities (e.g. bonds), and meta-statements about value relative to an instrument (e.g. derivatives). Prediction markets enable more nuanced and specific expressions about economic events, which in turn signal value more explicitly (along with risk) at both the macro and micro-economic level.

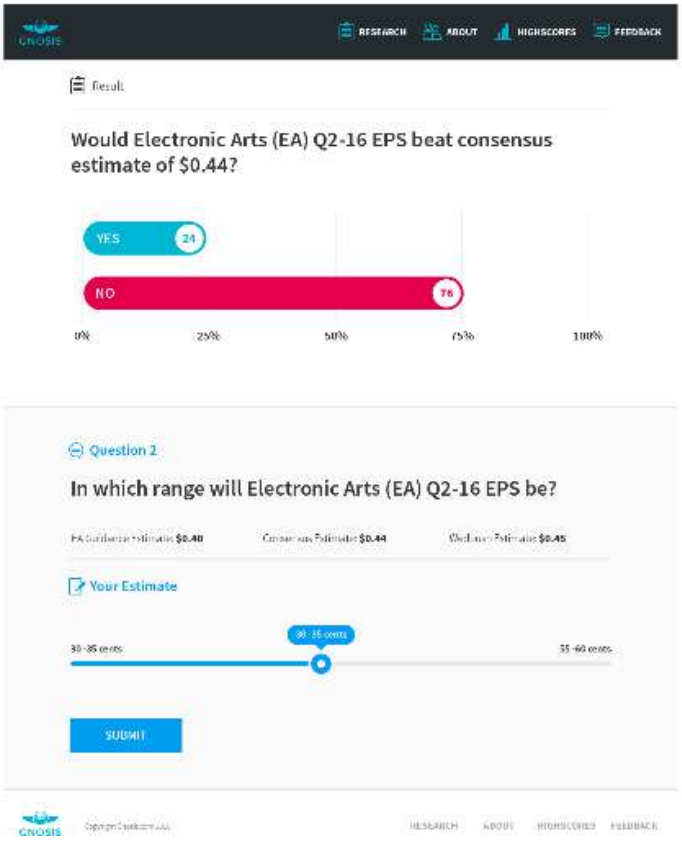

Figure 6.2: Financial Instruments: Predicting EPS .

For example, markets can be created asking, "What will this corporation's Q4 gross revenue be on a specified date?". One might imagine that information drawn from this and many adjacent markets could be used as an input to inform more advanced predictive/decision-making models in finance, government, insurance, and beyond. Such a market could inform analysts' earnings per share (EPS) estimates for the quarter; alternatively, markets can be constructed to predict EPS itself, sidestepping

the need for analyst forecasts altogether. More readily available and reliable information in this area can lead to better price discovery, minimizing both short-term volatility and long-term risk.

Alternatively, prediction markets can be used to create pegged and stable currencies. For example, an Ether/USD currency can be implemented by creating a scalar market which asks, “What will the Ether/USD exchange rate be at a future date?". Liquidity from this market can then be used to offer EtherUSD tokens which are pegged to the USD value. These tokens would be sold at a small markup dependent on the cost of the market to provide liquidity. In another case, stable currencies (currencies designed to have stable value) can be constructed by taking a basket of positions in both sides of many markets.
While these synthetic instruments seem somewhat complex in nature, they illustrate the diverse applicability of prediction markets in finance and represent a tremendous economic opportunity for a diverse set of local experts in a truly global environment.

The benefit of these types of markets is that they offer real-time access to all information relevant to a corporation’s value, leading to more accurate pricing and strong-form efficient markets. In the coming years, we will observe the interplay between new information markets and the incumbent financial system.

6.1.5 Insurance and Hedging Instruments

As stated previously, highly liquid prediction markets are remarkably accurate in assessing the likelihood of future events and therefore signaling associated risks. In the context of insurance, a prediction market could be used to estimate the likelihood of an insured event and may serve as an input to or even replace certain actuarial models. For example, a home insurance policy could create a market asking, “Will this area flood in the next year?” or “Will an earthquake over 5.0 magnitude occur within 50 miles of this location?”. Pricing outcomes from these markets with their attached probabilities can effectively approximate more sophisticated actuarial estimates that require highly specialized (i.e. expensive) training. In our case, risk measurement becomes democratized, creating new economic opportunities for any participants with valuable localized knowledge.

Insurances and hedging instruments have the common characteristic that they both reduce exposures to (financial) risks. Usually, with an insurance, many participants pay the insurer to take on their risk (the likelihood of occurrence being low but the financial damage being high).

Hedging involves making an investment that offsets the risks. For example, a farmer makes money in case the weather is sunny and s/he can farm her crops. If the weather is bad, s/he makes no money. To hedge risks associated with weather, s/he could strategically buy “NO” outcome tokens in the market “Will the weather be good?”. If the weather is good, s/he can farm her crops but loses in the prediction market. If the weather is bad, s/he cannot farm her/his crops but s/he receives the winning tokens in the market. S/he has effectively hedged her/his risks without the use of a middleman!

6.1.6 A countless number of use cases

In the above mentioned examples, we have outlined a fraction of many use cases. We see numerous possibilities to apply this forecasting technology and believe that it will revolutionize the current

pricing mechanisms as well as information gathering which will critically improve living standards. Applications ranging from “simple” markets to more complicated conditional markets can be built on top of the Gnosis platform.

6.2 Build Your Own

As a decentralized, permissionless platform, our goal is to make it as easy as possible for developers to build dApps on top of Gnosis. Whether you want to use prediction markets to predict climate change, govern a DAO, or build a flight insurance app, the range of relevant use cases is huge and we are excited to see them implemented by talented developers across the globe. We provide a DevKit to make it as easy as possible to build a use case of your own on top of the Gnosis platform.

6.2.1 Developer Kit

We are currently building a Developer Kit to make it as simple as possible to build your own use case with Gnosis. We will provide an environment in which you will be able to easily access everything needed to start coding. It will contain:

- The Ganache CLI, an Ethereum client which simulates a full client behavior, allowing you to run a “local blockchain".
- Gnosis.js, an easy-to-use tool to enable every website developer to build applications on top of Gnosis.
- GnosisDB, a generic database layer combining cheap storage with the advantage of fast document search and retrieval.

Interested in building your own prediction market with Gnosis? - Check our developer website as we will release our Gnosis DevKit very soon!

More information can be found under *https://github.com/gnosis*.

6.2.2 Gnosis X

Gnosis X is a recurring developer competition designed to encourage developers to build dApps on Gnosis. The aim of the challenge is to create an innovative and well thought prediction market use case on top of Gnosis. Through the year we will be announcing different categories which will be the main topics for the dApps. The participants will have at least three months to develop their application. Anyone can participate either individually or in a team. The submission will be judged by a jury consisting of Gnosis team members as well as changing blockchain and business experts. The dApps should strive to aggregate information, enable its free flow and carry a clear value-add for the designated category. To maximize the reach of the dApp it should be easy to use and have an appealing UI. The best application built on top of Gnosis will be rewarded with GNO tokens worth $100K. 40% of the prize will be distributed immediately after the winning dApp is announced. The remaining 60% will be released in the following 6 months after certain milestones are reached. We will offer dedicated developer support for participating teams. We highly encourage everyone interested in building a dApp on Gnosis to participate in our Development Incentivization program.

6.2.3 Gnosis Y

Gnosis Y will be an ongoing, open-ended developer program. It will focus on fundamental questions about the blockchain technology and prediction markets applications. Our long term goal is to support the community creating and promoting decentralized prediction markets on Gnosis.

7. Legal Consideration

Due to our aspirations for what Gnosis may one day become, the Gnosis team exercised extreme legal diligence in the lead-up to our launch. This diligence includes significant expenditures on several law firms around the globe to evaluate the implications of our structure, token launch, and operations. In the United States, we have worked closely with Perkins Coie. In our home jurisdiction of Gibraltar, we are working closely with Isolas and in Germany we are represented by Baker Tilly. We are actively seeking advice from regulatory bodies and are striving to shape Gnosis into what we hope is a model of regulatory compliance for decentralized applications and token launches. Due to the retrospective nature of regulatory action, the Gnosis team can make no guarantees that all our arguments will always eventually hold up in any given jurisdiction. As we have been in the past we will be responsive and collaborative with any regulators going forward: We fundamentally believe in the societal benefit of what we are doing and have no intention of flying under the radar.

7.1 Legal Implications of Token Launches

GNO tokens are functional utility tokens within the Gnosis platform. GNO tokens are not securities. GNO tokens are non-refundable. GNO tokens are not for speculative investment. No promises of future performance or value are or will be made with respect to GNO, including no promise of inherent value, no promise of continuing payments, and no guarantee that GNO will hold any particular value. GNO tokens are not participation in the Company and GNO tokens hold no rights in said company. GNO tokens are sold as a functional good and all proceeds received by Company may be spent freely by Company absent any conditions. GNO tokens are intended for experts in dealing with cryptographic tokens and blockchain-based software systems.

7.2 Legal Landscape for Prediction Markets

As discussed herein, prediction markets are an area of interest for many regulators around the globe, including those within the United States. Though we feel decentralization holds great promise, we must, and intend to, operate our business in accordance with the laws of relevant jurisdictions.

As such, Gnosis may not be immediately available in certain jurisdictions. The Gnosis team and several major law firms, which include Isolas and Baker Tilly among others, are resolutely pursuing strategies to bring the benefits of Gnosis and the information sharing economy to the globe as quickly as possible.

8. Leadership

8.1 Core Team

Martin Köppelmann, CEO

Martin Köppelmann has been an entrepreneur and thought leader in the blockchain space for more than 3 years. He co-founded the decentralized Gnosis prediction market - the first bigger dApp that went live on Ethereum. Closely related to prediction markets is his work on decentralized market driven governance mechanisms: Futarchy. Beyond the entrepreneurial activity Martin has done research on the economic incentive structure of different consensus mechanisms and scalability solutions via state channels. Martin co-hosts the Ethereum meetup groups in the Silicon Valley and San Francisco. Finally, Martin is well known for his work and research on "basic income on the blockchain: Circles" - a new currency built on top of Ethereum that aims to implement a basic income as monetary policy.

Stefan George, CTO

Stefan is an entrepreneur and developer who became interested in Bitcoin in 2013. Previously Stefan worked at tech companies in Silicon Valley and at Berlin-based startups. After finishing his Master's in CS he decided to travel Asia for a year in 2014 and started Gnosis afterwards working from Berlin. The first alpha version of Gnosis was released just one week after the launch of Ethereum. Stefan leads the development at Gnosis and implemented the smart contracts behind the prediction market platform.

Dr. Friederike Ernst, COO

Friederike is a physicist by training and after obtaining her PhD from the Free University of Berlin and subsequently conducted fundamental research at Columbia University and Stanford for a number of years. Friederike has moonlighted as a crypto technologist for many years and now structures and directs company operations at Gnosis full time. In addition, she is also the general secretary of the German Blockchain Association, the leading German thinktank on blockchain policy.

8.2 Board & Advisors

Joseph Lubin (Board member)

Co-founder of Ethereum and founder of ConsenSys. An academic background in Electrical Engineering and Computer Science from Princeton University and research experience in the field of Robotics Learning. Former VP of Technology at Goldman Sachs in the Private Wealth Management Division.

Jeremy Millar (Board member)

Chief of staff at ConsenSys. As Chief of Staff, Jeremy oversees many of the enterprise activities and strategic initiatives of the firm. Previously, Jeremy Millar was founder and managing partner of Ledger Partners. Ledger Partners developed out of Jeremy's increasing focus and passion for the blockchain and bitcoin ecosystem. This began with what was supposed to be a blog post that became arguably the most comprehensive report to date on what is happening in the world of bitcoin and blockchain startups, which you can see here: http://bit.ly/1Zq2Pvy. Jeremy began his career as one of the first Java architects at Oracle, before moving into sales management and strategy roles, both within Oracle and at a number of start-ups. He went on to complete his MBA at Oxford University before joining the M&A team at Goldman Sachs. Jeremy was a founding partner at Magister Advisors, advising fintech and SaaS companies across Europe. He is also an active angel investor and mentor with the Barclays Accelerator powered by Techstars.

James Slazas

20 years of capital markets experience, initially on the futures' exchanges of the CME and La Matif. Managed a proprietary derivative arbitrage and structured products book for Lehman Brothers. Also, held $1B in emerging market credit risk for Lehman's London, Swiss and Hong Kong banks for HNW clients. James managed a life settlement hedge fund uniquely acquiring longevity risk for limited partnership units.

Robin Hanson

Robin Hanson is an associate professor of economics at George Mason University and a research associate at the Future of Humanity Institute of Oxford University. He is known as an expert on idea futures and markets, and he was involved in the creation of the Foresight Institute's Foresight Exchange and DARPA's FutureMAP project. He invented market scoring rules like LMSR (Logarithmic Market Scoring Rule) used by prediction markets such as Gnosis, and has conducted research on signaling.

Jason Trost

Founder and CEO of Smarkets. Prior to founding Smarkets, Jason was an application developer at UBS's Global Asset Management (New York) where he focused on innovative web technologies. Jason founded internet startup Descipher, a consumer medical website and has also been an equities trader at Great Point Capital (Chicago).

Vitalik Buterin

Founder of Ethereum, Ethereum Chief Scientist. Vitalik Buterin is a Canadian programmer and writer primarily known as a co-founder of Ethereum and as a co-founder of Bitcoin Magazine. Vitalik helped to develop Gnosis' auction mechanism and is involved in the crypto-economic experiments conducted by Gnosis.