

Prediction markets

Analyst
Mrinalini Bhutoria (Ria)
@riabhutoria

Updated
13 November 2018

OVERVIEW

Prediction markets facilitate the trading of event derivatives. They have been around since the 1990s. They are sometimes also referred to as information markets, idea futures, and decision markets. Participants use prediction markets to speculate on outcomes of events. Many believe that decentralizing prediction markets will allow us to harness their full potential by lowering the cost of participating, bypassing strict regulation and increasing adoption by making the platforms more accessible across geographies.

There are multiple teams working on building decentralized prediction market platforms. We go over three of these projects below: Augur, Gnosis, and Stox. Augur launched its mainnet in July 2018, Gnosis launched its mainnet in December 2017 (though it is officially still in beta), and Stox is still in its beta phase.

Prediction markets use “the wisdom of the crowd” to determine the probability of a future outcome. The idea is that the collective wisdom of a diverse group of independent individuals results in more accurate and unbiased predictions than the prediction of an expert or small group of experts. Literature on the topic claims that while individuals have unique biases, gathering the knowledge and opinions of many individuals cancels out these individual biases, resulting in more robust and accurate predictions.

Till now, prediction markets have been centrally owned and operated. Some examples of centralized prediction market platforms include [PredictIt](#), Intrade, Betfair and DraftKings. A central entity operates the platforms, chooses markets to create, and resolves these markets. Users can buy and sell shares but cannot create or resolve markets. Critics claim that the central ownership makes these platforms unnecessarily expensive (fees range from 3% to 10% of profits) and potentially susceptible to manipulation.

Further, regulation is inconsistent from jurisdiction to jurisdiction (i.e. they are regulated as gambling in some countries and derivatives and options trading in others). No matter how they are regulated, the key similarity is that they are strictly regulated in most countries and run the risk of being shut down. Intrade was a popular prediction market platform, but was forced to exclude US participants in 2012, and [was shut down in 2013](#). The CFTC sued Intrade for “illegally facilitating the sale of futures contracts”, which can only be traded by special exemption in the United States or on a registered exchange. In the US, sports betting was illegal outside the state of Nevada until recently. A [Daily Mail article](#) from April 2015 outlined that 90% of all sports betting was carried out illegally. In May 2018, the [Supreme Court](#) ruled that states could choose to legalize sports betting in their respective states. This type of regulatory scrutiny has prevented prediction markets from gaining mainstream attention or adoption beyond gambling and betting.

However, prediction markets could be a powerful forecasting tool. The Iowa Electronic Market (IEM) is a group of real money prediction markets operated by the University of Iowa. IEM is not-for-profit and was created purely for research and education purposes. Compared to major opinion polls on US elections, forecasts by IEM prediction markets outperformed 451 out of 596 times. Before the results of the 2004 elections were announced, IEM predicted George W. Bush would get 51.45% of the vote and John Kerry would get 49.55% of the vote. The actual results were Bush with 51.56% and Kerry with 48.44%. Prediction markets have also proven more accurate than surveys in forecasting payrolls, unemployment claims, retail sales, business confidence, and other macroeconomic indicators and have reduced forecast error by 5% on average.

¹ Wiser: Getting Beyond
Groupthink to Make Groups
Smarter

In addition, a number of corporations have used internal prediction markets to improve their forecasts. For example, HP's prediction market forecasts were 70% more accurate than HP's traditional forecasts in the price of computer memory three and six months ahead. Best Buy has used prediction markets to forecast the demand for digital set-top boxes, store opening dates, and to determine whether new services will be launched on time². Google also launched internal prediction markets, allowing employees to place "bets" on when products would launch and their success. Google's prediction markets have also been accurate in predicting the events, as employees with private information share the information in the form of buying and selling outcomes, without having to disclose the information.

This is a key feature of prediction markets. Participants are incentivized to act on private information (and reap the benefits) without needing to publicly disclose the actual secrets or information. Also, participants have real money at stake, which provides a financial incentive over surveys and polls.

Decentralization - Benefits

- Decentralization could improve reporter accountability³, establish censorship-resistance, engender global participation and user diversity, and encourage healthy competition.
- Proponents believe that reporter accountability improves with decentralization because there is a hard-coded protocol for users to challenge inaccurate reports and punish malicious reporters who report incorrectly. The resolution processes happens openly according to a well defined contract.
- Decentralization enables global participation because open blockchain platforms do not discriminate between users from different regulatory jurisdictions. This expands the user base and creates greater diversity in thoughts and opinions. By incorporating a wider variety of opinions, prediction markets can be more accurate by eliminating bias specific to individuals or small groups of individuals.
- Censorship resistance is important because it prevents central entities with power from censoring and shutting down markets. This has its negative consequences as well, such as malicious markets and lack of investor protection for participants who have minimal trading experience.
- Healthy competition among market creators could result in lower market creator fees. The idea is if the market creator fee for a specific market is high, another market creator can win over users by launching the same market with a lower market creator fee.

Decentralization - Challenges

The downside of decentralization stems directly from the lack of regulation or accountability beyond the blockchain. The owners of a centralized entity that is regulated risk losing their business, financial loss, reputation, jail-time, and more. The penalty for dishonest behavior is greater for a centralized entity than a participant in a decentralized network. Although decentralization allows for global participation in prediction markets, they are currently unregulated and there is no regulatory recourse or protection in place for participants who are by creators and reporters.

Another challenge with crypto-based prediction markets is volatility of tokens. Users have to be willing to convert across multiple currencies to participate. The flow as it stands is local currency -> USD/EUR/GBP -> ETH -> Native token (i.e. REP, STX, GNO, etc.) Transaction -> (i.e. REP, STX, GNO, etc.) -> ETH -> USD/EUR/GBP -> Local Currency. This is expensive, complex and requires users to assume multiple layers of FX volatility, which could deter the use of decentralized prediction markets. We go over additional challenges in the "General Challenges" section below.

Despite these risks, many believe that the benefits of decentralization are worth the risks and will expand the addressable market, thus improving the accuracy of forecasts and predictions.

² blog.gnosis.pm/the-power-of-prediction-markets-fedea0b71244

³ The caveat here is that malicious reporters are only accountable to the extent they lose tokens they have staked. A centralized entity that is regulated risks losing their business, financial loss, reputation, and more. Thus, it seems that the incentive to be honest is greater for a centralized entity than a reporter in decentralized networks.

Addressable Market

While there have been a few attempts at sizing specific verticals, the figures vary drastically and there is no good estimate of the total addressable market for prediction markets. It is challenging because a good portion of trading supposedly occurs illegally, under the radar. [A Wired article](#) claims that the size of wagers in illicit sports betting ranges from \$80b to \$150b annually, whereas [a Daily Mail article](#) sized just the global sports betting market at up to \$3 trillion in 2015.

TYPES OF MARKETS

Prediction markets have at least two outcomes. They can be binary (yes or no), categorical (who will win the World Cup?) or scalar (What will the price of FB be on December 31, 2018?). Categorical markets can have multiple outcomes. Using the World Cup example, choices could be a) France b) England c) Germany d) Argentina e) Brazil, etc. Scalar markets have two outcomes - long (the price will rise) and short (the price will fall). Augur, Gnosis, and Stox all have different ways of implementing scalar markets.

According to a [February 2018 presentation](#) by Tom Kysar of the Forecast Foundation, the payout in a scalar market on Augur will be correlated with the final value such that holders of “long” outcome shares will be paid more when the value is higher and holders of “short” outcome shares will be paid more when the value is lower. In scalar markets, the payout could be divided between holders of long and short outcome tokens, unlike in binary and categorical markets, where the entire payout goes to holders of a single outcome token.

PREDICTION MARKET USE CASES

Although the most obvious use cases for prediction markets are gambling and betting, prediction markets’ ability to aggregate the collective wisdom of the crowd to determine the probability of an outcome extends the use cases beyond betting.

Global participation in markets

Decentralized prediction markets could allow participants to gain exposure to events or assets they aren’t able to trade easily or at all. Consider middle class citizens in third world countries who want to trade shares of U.S. based stocks. Currently, in many countries, they are incapable of participating because of capital controls that make it too expensive. Decentralized prediction markets could allow such participants to gain exposure without having to pay excessively high fees to bypass regulatory controls. Theoretically, a middle class citizen in China can now get exposure to Apple stock by buying shares in the prediction market “What will the share price of Apple be at the end of 2018?”

For investors in countries with capital controls, a tool that could allow them to access the American or EU market exposure could be attractive. Even with the volatility inherent in an ETH-based dApp, the opportunity to gain exposure to previously restricted investment assets could prove to be a huge draw, as users gain long or short exposure to price movements via synthetic contracts.

Forecasting

Another prediction markets use case that has been discussed by advocates is using markets as a forecasting tool. In theory, characteristics that make prediction markets more efficient and accurate over other forms of forecasting are that they efficiently aggregate a large amount of information, beliefs, and data. They obtain *truthful* data and realistic beliefs through the use of financial and other incentives. Finally, new information is quickly integrated and reflected in the price. In practice, political campaigns could create a prediction market and avoid hiring a team of pollers to make individual phone calls, thus saving significant time and money.

Some experts believe that using prediction markets internally within a corporation could result in more accurate forecasts. The idea is that more employees are more inclined to share information when they are kept anonymous and when they don’t have to disclose the exact information. Examples of companies that have used prediction markets include HP, Siemens, Best Buy, Chrysler, Intel, Microsoft, and [more](#). However, one challenge could be risk of market manipulation by stakeholders who have a lot to gain or lose - i.e. the last thing a corporation needs is the IT department vying for a particular product launch to be delayed.

Hedging

The entire insurance process could be automated using smart contracts. Companies heavily exposed to a particular type of natural disaster (i.e. earthquakes, hurricanes, or wildfires) could buy shares in outcome “yes”. If the natural disaster occurs, their payout could offset payouts they would have to make in claims or damages to plan members.

Hedging is an example of self-insurance and a widely discussed use case for prediction markets. Anyone can use prediction markets to hedge their positions and limit their downside. A common example is farmers hedging their exposure to weather conditions. Farmers relying on rainfall could protect themselves from financial loss in case of drought by creating a prediction market around “will there be rainfall?” and buying a small amount of outcome “No” shares.

The caveat that prevents skeptics from believing in hedging as a popular use case is the layers of volatility we discuss above, which, if not managed correctly, would lead to more harm than good.

Futarchy

Futarchy is market based governance process that can be applied to governments, corporation, foundation, and DAOs. Futarchy was developed by Robin Hanson, who has worked in the field of prediction markets for over 20 years. He is also the mind behind the logarithmic market scoring rule (LMSR). Futarchy was born from the idea that a lot of the barriers to making good decisions (especially political and corporate) lie in not knowing answers to key questions.

Say the government needs to make a decision on whether they should fund an infrastructure project. Two markets can be created, “what will the GDP be in a year if we fund this project?” and “what will the GDP be in a year if we do not fund this project?” These markets can be traded for a specified period and at the end of the period, one market will have a higher estimate for what the GDP will be under that decision. The government would implement the decision that corresponds with the higher GDP estimate.

Barriers to adoption. A key challenge with Futarchy is achieving consensus on the correct metrics and time period to create markets and base policy decisions around. In addition, Futarchy based organizations could be susceptible to market manipulation - people who are at risk of being negatively affected by a specific policy decision could manipulate the markets by buying a large amount of shares in the outcome that would negatively affect them.

Dynamic betting

In traditional betting, participants wait until an event occurs and cannot change their position based on new developments leading up to the event. Prediction markets, on the other hand, allow participants to buy and sell predictions up to event occurrence. This allows them to change their predictions and positions as they uncover new information.

For example, consider the market, “Will the Eagles win the Super Bowl?” Participants may believe this is true now and buy shares in outcome “Yes”. However, suppose their quarterback gets injured a week prior to the Super Bowl. They may no longer believe the Eagles will win. They could sell their “Yes” shares and exit their position or exchange their “Yes” shares for “No” shares.

Augur (REP)

OVERVIEW

Augur is a decentralized prediction market built on Ethereum that allows users to create and trade outcomes of events in any category. Augur rewards users for correctly reporting events and penalizes them for incorrectly predicting or reporting on events. Its native token is called REP (short for Reputation), which Augur claims it needs to secure the network. According to one of its founders, Joey Krug, Augur is currently the largest dApps built on Ethereum - it has over 100 contracts and ten times more code than the next most complex contract (MakerDAO).

Joey Krug, Jeremy Gardner, and Jack Peterson are the co-founders of Augur. They began working on the project in late 2014. Initially, the team used a programming language called Serpent to build the platform. The team rebuilt the platform in 2017 using Solidity due to major flaws and vulnerabilities with Serpent. Augur was founded under parent company, Dyffy, Inc., but is now under the purview of the Forecast Foundation. The Forecast Foundation is a non-profit legal entity in charge of the development and promotion of Augur. The members write code for Augur and contribute to the code base. They claim they don't have the power to censor the platform.

The value of an outcome share represents the market estimated probability of the outcome. For example, a share price of 0.45 ETH means the market expected probability is 45%. Price/probability fluctuates as market participants discover and price in new information. When users buy shares, they are effectively entering into a contract with someone taking the opposite side of the bet. Whichever party holds the correct outcome share collects the combined amount of ETH put into the contract by both sides. The sum of the price of shares of all outcomes equals 1 (or 100%). The party with the incorrect outcome share loses the ETH placed into the contract.

Augur allows participants to create a market for any event that has an outcome that can be verified with real world information. Events can include, but are not limited to, political elections, sporting events, financial results, natural disasters, etc. Once a market is created, traders can then buy and sell shares in each of the outcomes from market creation until market close. Upon market close, reporters report on the outcome of the event by staking REP tokens. We go over the entire process and accompanying caveats in detail below.

We look at Augur through the binary market lens. Users can also create categorical markets (events with more than two outcomes) and numerical markets or scalar markets (with two outcomes - long and short).

AUGUR PREDICTION MARKET: FOUR STAGES



Creation

Anyone can create a market about any upcoming event. The creator must select an end time, a creators fee (paid to the creator by traders to compensate them), a designated reporter (creators can designate themselves as reporter), and a resolution source. Market creators can set a creators fee between 0% to 50%. Even though the upper limit is so high, Augur claims competition among market creators will keep the creator fee low, as there are very low barriers to creating markets. Market creators can also provide initial liquidity to attract users to their market by taking the opposing side of the order if there is no one else to do so. The shares are placed on the order book at the time of market creation.

The creator must also post two bonds at the time of creation, the validity bond (in ETH) and the designated report no-show bond (in REP). The validity bond is returned if the finalized outcome is anything but invalid. This is used to incentivize creators to create markets with clear outcomes. The no-show bond is returned to the market creator if the designated reporter (DR) shows up to report within three days of the market's end date. If the DR does not show, then the first public reporter to accurately report receives the no-show bond. This reporter does not have to stake any REP in this case - the no-show bond fulfills the staking requirement.

The size of both bonds are set dynamically based on the proportion of invalid markets and the proportion of failed designated reporters, respectively. The market creator also needs to pay gas, which is the cost paid to Ethereum miners to process the market creation transaction.

Platform risks associated with Ethereum could prevent the no-show bond from fulfilling the intended purpose. For one, due to congestion on the Ethereum network (see [here](#)), the market creator could lose the no-show bond if it takes more than three days to add the Ethereum transaction containing the reported outcome to the blockchain. Another way the market creator could lose the no-show bond would be if the designated reporter experiences a DOS attack⁴.

Trading

Augur allows participants to buy and sell shares of different outcomes associated with a market event from the time the market is created till it is resolved. Participants do not need to own any REP in order to trade. Participants can input how many shares they want to buy and the max amount they're willing to spend (limit order). The limit price must be between 0 and 1 ETH. Participants can also buy portions of shares.

The image shows a trading interface for Augur. At the top, there are two tabs: "BUY" (selected) and "SELL". Below the tabs is a horizontal bar with a green segment on the left. The main form contains the following fields:

QUANTITY	0.0001
LIMIT PRICE	0.4
<input type="checkbox"/>	FILL ORDERS ONLY

At the bottom of the form, there is a summary line: **EST. COST 0.00004 ETH**

Augur has an automated matching engine that exists within Augur's smart contracts. Trades are filled immediately if there is a matching trade on the order books. Trades may be executed by buying shares from/selling shares to other participants. The Augur team claims that trades are revealed a block later to prevent miners from front-running participants. This is misleading - even if the Augur contracts hide the values through a contract function, any full node has direct access to the memory and can read the storage directly because the EVM compiler has strict rules about where the state is stored. If there is no matching order or the order can only be partially filled, the remainder is placed on the order book as a new order. These can be removed from the book at any time by the creator.

⁴ The attacker could launch a DOS attack by flooding the Ethereum network at large or launch a DOS attack specifically against the designated reporter's geth node and temporarily block the reporter from the Ethereum network. In both instances, the DOS attack would prevent the DR from reporting on time. The attacker would then have the opportunity to become the first public reporter. It is unclear if Augur has any safeguards against such an attack.

ORDER BOOK		
ASK QTY	PRICE	DEPTH
5.0000	0.6439	35.4900
1.0000	0.6430	30.4900
1.9000	0.6300	29.4900
5.0000	0.5851	27.5900
21.9900	0.5710	22.5900
0.6000	0.5550	0.6000
0.5025 ETH		
6.0000	0.4500	6.0000
4.9995	0.4251	10.9995
208.7486	0.4137	219.7481
0.2000	0.3395	219.9481
0.1000	0.3000	220.0481
10.0000	0.1000	230.0481
BID QTY	PRICE	DEPTH

Consider the market event “Will bitcoin’s price reach \$20,000 by December 31st, 2018?”. The market has two outcomes - yes (buy) and no (sell). You believe this is true and want to buy shares. One way to do so is to buy shares from another participant who is selling the shares they own. You give them between 0 to 1 ETH per share and they give you the shares. Now you own the share, while they have exited their position. Alternatively, you can find someone who wants the opposing share as you. You both go to Augur together and put in some portion each (i.e. you put in 0.6 ETH for yes and your counterpart puts in 0.4 ETH for no). Together, you buy what is called a complete set from Augur (one of each outcome) for 1 ETH. When the market finalizes, one of you will have a share that is worthless and the other one will have a share that is worth 1 ETH (minus fees). Both scenarios are hidden from the users in the UI but this is how things work under the hood. Users just need to choose an outcome and specify their limit price and number of shares.

One of Augur’s limitations right now is that every transaction a user conducts must be broadcasted to the Ethereum blockchain and processed by its miners. However, the team has mentioned a potential integration with 0x, which enables partially off-chain trading. In theory, the integration would allow users to create, modify, and cancel orders faster without having to post each transaction to Ethereum.

The counterparty in the above example believes the answer is no. On the Augur platform, in a binary market, selling “yes” shares is equivalent to buying a “no” share, but the platform is set up such that users buy or sell an outcome in binary markets. Thus, you don’t buy “no” shares. Users who are short “yes” (long “no”) can buy “yes” shares if they want to settle and exit their position before the market closes and determines a winning outcome.

Settlement

There are two ways to settle. Participants can sell the shares they own on the market for ETH. Augur handles this by matching orders through its automated matching engine. Traders can also hold their shares and receive payout upon market finalization, if they are long the correct outcome. If they are not, they receive no payout and lose their investment.

Traders also have to pay settlement fees, which consist of the creators fee and the reporting fee. Unlike the creator fee, the reporting fee isn’t set by anyone. It uses an off-Augur price feed (i.e. coinmarketcap) to determine the REP price and market cap. Then the Augur engine calculates the appropriate reporting fee needed to guarantee the integrity and security of the platform using the current market cap and open interest on Augur.

The reporting fee formula is $Current\ Reporting\ Fee \times [(Open\ Interest \times 7.5) \div Market\ Cap]$. The reporting fee is adjusted once per fee window, which is once every 7 days. Settlement fees are collected anytime settlement occurs

i.e. when selling a complete set or redeeming shares in finalized market.

Outcome Probability

The equilibrium price associated with an outcome ($0 \text{ ETH} < \text{Price} < 1 \text{ ETH}$) reflects the market expected probability that outcome will occur. The price of outcome shares fluctuates based on supply and demand. As more people participate, the accuracy of the prediction supposedly improves because greater participation cancels out individual bias, if participants are diverse and independent. Augur outlines different bid and ask trades, payouts, and fees [here](#).

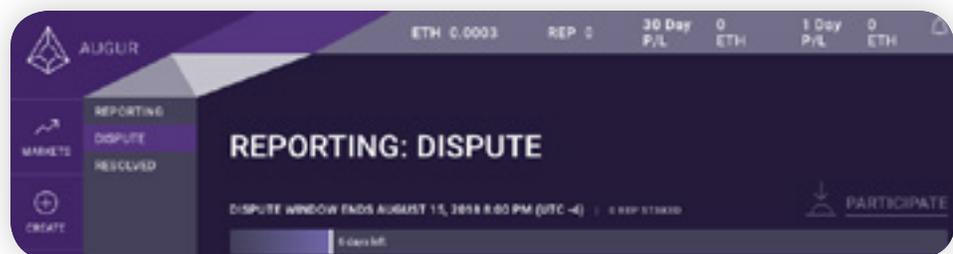
REPORTING

Reporters (or Augur's oracle⁵) are a key component of the Augur ecosystem. Any REP token holder can be a reporter and token holders are incentivized to report. In order to report, participants need to stake (lock up) REP with Augur. If they report incorrectly, participants lose their stake. This is to incentivize them to report accurately. The outcome that receives the most votes (implicitly if no disputes or explicitly if disputed) from reporters becomes "consensus" and is considered the tentative outcome. If reporters resolve markets correctly, the staked REP is returned and reporters are rewarded in reporting fees.

Reporting fees are set dynamically and collected during the 7-day reporting period following the market close date. The reporting fee is built into market creation and is calculated based on the market cap of REP. Reporting fees are denominated and paid out in ETH. There are three ways to earn reporting fees: 1) staking REP during the initial report, 2) buying participation tokens, and 3) disputing a tentative outcome.

Participation tokens

Augur offers participation tokens to reporters who may not need to report on or dispute an outcome during a given fee window. Participation tokens are used as an incentive to encourage users to show up during a fee window in case their participation is needed during a fork state. Participation tokens are not tied to a specific market or event. Users can buy participation tokens with REP. At the end of the fee window, the REP they used to buy participation tokens is returned to them. They also earn reporting fees proportionate to the participation tokens they purchased. Users can purchase participation tokens at any time during a fee window (every week).



Reporters have the ability to dispute the tentative outcome during the dispute round, which lasts 7-days following the determination of the tentative outcome. Disputing the tentative outcome requires reporters to stake REP on an outcome other than the tentative outcome. Suppose a market event has outcome "yes" and outcome "no". The tentative outcome is outcome "yes". Outcome "no" and "invalid" have a dispute bond requirement and a chance of becoming the winning outcome if the dispute bond is filled. If the total amount of dispute stake meets the dispute bond size, the dispute is successful.

The dispute bond size is chosen such that reporters who successfully dispute a false outcome receive a 50% ROI. Dispute bonds can be funded by multiple participants. This is useful if a market undergoes multiple dispute rounds, resulting in a large dispute bond requirement⁶. If any outcome that is not the tentative outcome receives enough dispute stake from one or more users to fulfill its requirements, then that outcome becomes the new tentative outcome. The new tentative outcome will either undergo another dispute round (lasting another 7-days) or enter a fork state. Dispute stake is returned if a dispute is unsuccessful (i.e. if there is not enough stake to fill the dispute bond size associated with a particular outcome). All users who contributed to the dispute bond will also get a proportional reporting fee from the fee pool (successful or not). A market enters the fork state if the filled dispute

⁵ An oracle is an external actor or entity that feeds information from the real world into the blockchain.

⁶ The dispute bond requirement increases with each new dispute round.

bond is greater than 2.5% of all REP. If no dispute bond is filled by the end of the 7-day dispute round, then the tentative outcome becomes the winning outcome.

Fee window. The fee window is synonymous with the dispute round, which is continuous and lasts 7-days per round. Fees collected during the fee window are added to the reporting fee pool. The pool is used to reward token holders that participate in some way during the fee window.

Fork state

If the dispute bond/stake in any market exceeds 2.5% of total REP, the entire Augur system enters the fork state. It is seen as the last resort and structured such that participants are deterred from allowing the platform from getting to that point because it is very disruptive. The fork state lasts 60 days to give token holders, wallets, and exchanges enough time to prepare.

The original universe in which a market is created is called the parent universe. The forked market creates a different universe for each possible outcome. These are called child universes. A binary market (yes/no) would have three child universes - yes, no and invalid. During a fork, the parent universe becomes permanently locked. No new markets can be created, no markets can be finalized, and no fees can be paid out. Shares can be traded and there can be initial reports, but in order for them to mean anything, token holders must migrate REP tokens to a child universe.

REP tokens cannot be transferred across child universes. Once they are transferred to a specific child universe, the move is permanent. All REP staked on non-forking markets is unstaked so holders can move them to a child universe during the 60-day period. Whichever child universe gets the most REP becomes the winning universe, and its outcome becomes the winning outcome. This final outcome cannot be further disputed. Unfinalized markets can only be transferred to the winning universe. If they have received initial reports, they enter the “waiting for next fee-window” to begin.

Token holders are incentivized to migrate their tokens to a child universe because they receive an additional 5% REP in that universe. Users can migrate from parent to child even after the 60-day period, but their tokens don't count in determining the winning universe and these users forgo the 5% REP reward for migrating during the fork state. Reporters that have staked tokens on one of the token market outcomes cannot change their position during or after the fork i.e. it is not possible to migrate tokens across child universes.

Because the child universes are mutually exclusive, REP tokens that exist in one child universe can't be used in another child universe. The idea is that REP tokens in universes that don't correspond to objective reality would be worthless as nobody would want to participate in prediction markets with an untrustworthy oracle that doesn't resolve markets correctly. Augur believes that the threat of forking is enough to prevent the network from actually forking. As participants know that forking process will ultimately establish the truth, the idea is that the threat of a fork and the use of incentives will drive honest behavior.

Parasitic markets. Parasitic markets refer to markets that are derivatives of Augur markets but don't charge any fees. In short, in order for REP to remain secure, the network needs to know the total value at risk (open interest) to accurately assess REP's market cap in order to effectively secure the open interest at any given time. Total open interest equals to $I_a + I_p$. Augur can know the internal open interest (I_a) but it does not have a way to know external open interest (I_p). Thus, Augur must make an assumption about I_p . However, if Augur's assumption about the open interest on parasitic markets is greater than expected such that the minimum cost of launching an attack is less than the maximum profit then the security model could break.

In response to a question on [Stack Exchange](#), Augur has mentioned that the tentative plan is to closely monitor the system at launch. It is possible that internal open interest (or I_a in the equation above) will be greater than derivative or parasitic open interest.

A centralized parasitic market mints money for the operator and the fees are likely to be lower for the parasite because it is all centralized. If parasitic open interest surpasses internal open interest, then the Augur team has suggested that they could coordinate with creators of parasitic markets off-chain through human interaction and convince them to convert parasitic markets to internal markets and pay the fees, which Augur claims will be very low. However, it is not guaranteed that this method will work, so parasitic markets continue to pose a

⁵ An oracle is an external actor or entity that feeds information from the real world into the blockchain.

risk without a clear cut solution.

Launching an Attack. Augur aims to make it such that the maximum benefit to launch an attack is less than the minimum cost of doing so, though it faces a few challenges in doing so. According to Augur, the maximum benefit to an attacker equals open interest on Augur (Ia) and on Augur's parasitic markets (Ip).

Augur can determine what the target REP market cap should be in order to secure the network. If the market cap is above the target, Augur automatically lowers reporting fees. If the market cap is below the target, Augur automatically increases reporting fees.

The caveat is that Augur cannot know the open interest on parasitic markets with certainty, so it makes an assumption. This means that Augur can never be objectively certain that the network is secured against attackers. Further, the reporting fee is adjusted once per 7-day fee window. Thus, if the market cap goes above/below the target market cap, the network may be vulnerable until the fee is adjusted. Augur believes if that occurs, market participants will buy or sell REP in anticipation of the reporting fee rising or falling, driving the market cap closer to its target and compressing the vulnerability window even further.

TOKEN FUNCTION

REP is an ERC-20 token and is the native token of the Augur protocol. REP stands for "reputation". There are multiple ways the Augur protocol utilizes the REP token.

Staking

The main function of the token is for staking. In order to report an outcome, token holders must stake or lock up REP tokens. This is to provide a financial incentive to participants to report correctly. If they don't, they lose their stake. Market creators must post no-show bonds in REP to incentivize them to choose a reliable designated reporter that shows up (or to incentivize them to show up if they are the designated reporter). In the case of a dispute, participants must contribute to the dispute bond in REP tokens - this refers to their dispute stake.

Token holders can also stake REP tokens by exchanging REP for participation tokens to earn fees from the reporting fee pool in proportion to the REP they staked, if they don't need to report or dispute an outcome during a given fee window. Finally, token holders use REP tokens in a fork state by migrating their tokens to the child universe corresponding to the outcome they believe is correct. They are incentivized to migrate tokens during the 60-day period because they are rewarded an additional 5% in REP tokens in the child universe to which they migrate.

Governance

The Augur community has mentioned that token holders may be able to use REP tokens to vote on future software changes. As of now, the team has indicated that the weight of their vote would be proportional to their stake of REP tokens.

AUGUR-SPECIFIC CHALLENGES

Infighting and legal troubles

The Augur founders were involved in a civil lawsuit filed by alleged co-founder Matt Liston, who was seeking \$152 million in damages. According to the lawsuit, angel investor Joseph Ball Costello and co-founders Jack Peterson, Joey Krug, and Jeremy Gardner "committed acts of fraud, breach of contract, trade theft and coercion," failed to recognize Liston as co-founder of the project and failed to allocate Liston a stake in the Augur ICO. This lawsuit is the most financially significant lawsuit in the crypto space.

Krug denied the claims outlined in the lawsuit and [said](#), "The claims are baseless and inaccurate. He [Liston] accepted a cash severance payment and he signed a full release with Dyffy and we're appalled that he's turned around with a lawsuit three years later. There hasn't been a single GitHub commit by Liston, on any of the Augur repositories. He's not a founder of Augur."

The lawsuit was filed in May 2018 and the hearing was scheduled for September 2018. According to [records](#), the lawsuit between Matt Liston v. Joey Krug, Jeremy Gardner, and Jack Peterson has been dismissed by the court (on October 12) and is being settled outside the court. Details around the settlement and how much

participants had to pay in legal costs in the process are unclear.

User experience

Compared to centralized applications, Augur has a ways to go in improving the user experience. The team enlisted design consulting firm, IDEO, to help build the user interface, but the application has multiple challenges it needs to overcome. The web application is slow - downloading it takes time (~30 minutes) as you have to sync with the mainnet when you initially download the application. It also requires the user to quit and restart the app a few times before it is fully synced and ready to use. If the application isn't left open, users have to sync with the mainnet every time they open the application before it launches. Users also need to have a Metamask, Edge, Ledger or Trezor account in order to use the application. Further, Augur does not have a working mobile application. From the very beginning, users are aware that they are using a dApp. The idea is to get dApps to a level such that the quality of the dApp user experience is just as high as the centralized counterparts.

⁵ An oracle is an external actor or entity that feeds information from the real world into the blockchain.

Gnosis (GNO)

OVERVIEW

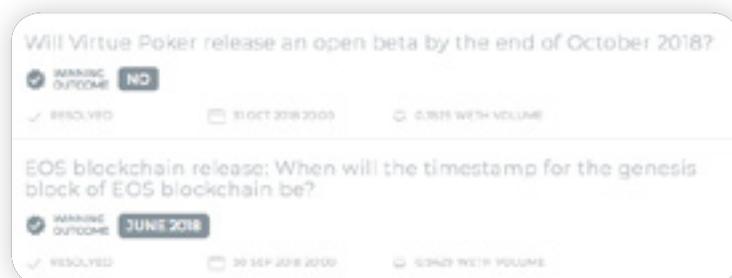
Gnosis is a decentralized prediction market platform being built on Ethereum. Gnosis joined Consensys as its first “spoke” in January 2015, and was spun out in March 2017. Since its founding, Gnosis has expanded into new products and services aimed at complementing its prediction markets platform. Gnosis also provides third party developers with tools to build new prediction market applications on top of Gnosis because the team believes that different categories of prediction markets should have different trading interfaces and different marketing and regulatory strategies.

The additional products include two wallets (Gnosis Multisig and Gnosis Safe), a developer toolkit (Gnosis Apollo), and a decentralized Dutch auction based exchange (DutchX). The Gnosis prediction market platform uses two tokens - GNO and OWL. The main function of GNO is to generate OWL tokens and the main function of OWL tokens is to pay trading fees. The native token of DutchX is the Magnolia token (MGN).

Product/Service	Description	Status
Gnosis Trading Interface Beta	The management interface is the actual prediction market platform for users to trade in prediction markets. It is live on the mainnet.	Released end of 2017
Gnosis Olympia	Olympia is a “tournament” or a test version of the prediction market platform that allows participants to try out trading in prediction markets.	First tournament held end of 2017
Gnosis Apollo	Package that provides tools needed for companies to run decentralized prediction market tournaments for their own purposes	Released May 2018
Gnosis Multisig	A wallet that holds ETH and ERC-20 tokens, integrates with web3 wallets (e.g. Metamask), supports offline signing, hardware ledgers, owner configuration and specification of signatures.	Released
Gnosis Safe	A wallet geared towards single users using two or more factor authentication, which can be held by phones, tablets and hardware ledgers.	Released 1Q18
DutchX	DutchX is a decentralized trading platform for ERC-20 tokens using the Dutch auction mechanism to determine a fair value for tokens.	Released July 2018

Gnosis Olympia

Gnosis Olympia is an alpha version of the prediction market platform. It provides participants with an environment to test trading in Gnosis prediction markets. Participants use play OLY tokens and can win GNO tokens for successful predictions. Gnosis held the first round of the Olympia tournament for a two week period from December 18, 2017 to January 5, 2018. The tournament featured 22 prediction markets. The second tournament was held exclusively for Dappcon attendees from July 19-20, 2018. The third tournament was held from September 7-9, 2018, during ETHBerlin.



Sample Olympia Prediction Markets (12/18/17 to 1/5/18)

⁷ ConsenSys is a venture production studio building decentralized applications and various developer and end-user tools for blockchain ecosystems focused on Ethereum.

Apollo

Gnosis released the Apollo package to make the creation of customized prediction market applications on top of the Gnosis platform easy for individuals and enterprises. Gnosis recently launched GnosisX, a competition with a monetary reward to encourage developers to build vertical specific prediction market interfaces on the Gnosis platform.

DutchX

DutchX is a decentralized Dutch auction based exchange for ERC-20 tokens. Buyers submit their bid at the point in time where the current price reflects their maximum willingness to pay until the auction closes. Gnosis believes a Dutch auction is an effective way to determine a fair price. Every buyer receives their tokens at the closing time for the same price.

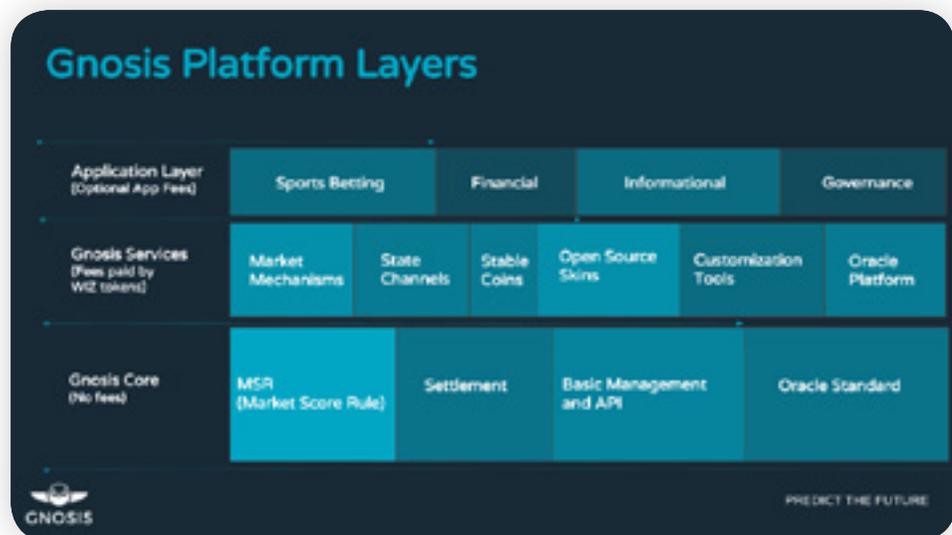
Token Sale

Gnosis held a token sale in April 2017. The sale was structured as a modified dutch auction - everyone who participates pays the last price. The sale was set up such that it would end when 9 million GNO tokens were sold or when the funds raised reached 250K ETH, whichever came first. When the sale actually took place, Gnosis raised 250K ETH within 15 minutes for 5% of the total supply. Gnosis has been criticized for the way the token sale was conducted because the team ended up with 95% of the token supply following the token sale. Gnosis currently has 200,000 ETH in reserve.

GNOSIS STRUCTURE

Three Layers

In addition to providing users the ability to create prediction markets, Gnosis also provides tools to developers to build their own prediction market applications and divides the platform into three layers. Most of the functions on the first layer (Gnosis Core) have no fees. The second layer, Gnosis Services, allows providers to charge fees for using the services offered. The third layer, Gnosis Applications, could have fees based on the model of the applications built on this layer.



Core

The first layer is known as Gnosis Core. It is open source and mainly free to use. This layer provides the smart contracts needed to create prediction markets. The two key components are the event and market mechanisms. The event contract allows users to create and resolve markets. It includes an oracle, outcome tokens, and collateral tokens. The only process that incurs fees (other than gas costs) is the creation of outcome tokens. The max fee is 0.5% and is paid by traders buying the tokens from market makers. Every event contract is connected to an oracle. Every event contract has at least two outcome tokens. Outcome tokens are ERC-20 compatible tokens.

Collateral tokens refer to the token in which the market is denominated. For example, a participant may deposit ETH to buy a set of outcomes, making ETH the collateral token.

The market contract allows participants to trade outcome tokens. Market contracts are not required but Gnosis claims that market contracts improve liquidity and usability. Market creators must provide initial liquidity to the market contract in the form of collateral tokens. Market contracts have an automated market maker. Once the market starts trading, the automated market maker then buys and sells shares of outcomes at a price determined by an algorithm given the current state of the market. The pricing mechanism that Gnosis uses is the Logarithmic Market Scoring Rule (LMSR) - more on this below. Market creators charge an option fee for providing this initial liquidity by charging a fee in the form of a spread between the bid and ask price.

Users can also buy and sell outcome shares to other participants once enough complete sets have been created. From what we understand, the exchange of shares is conducted on DutchX, Gnosis' decentralized Dutch auction-based exchange.

Logarithmic Market Scoring Rule (LMSR). Gnosis has implemented an automated market maker, a bot that prices outcomes based on the Logarithmic Market Scoring Rule (LMSR), within the market contract framework. With LMSR, the price varies based on the supply and demand of outcome shares. The greater the volume and liquidity on a market, the larger trade volumes would have to be in order to cause a large shift in the price of shares. LMSR tries to price outcome shares depending on how abundant (price is less) or scarce (price is more) they become. By utilizing LMSR, Gnosis aims to tackle the challenge of liquidity in prediction markets. Unlike traditional financial markets, prediction markets have less participation, volumes, and thus liquidity at the time of writing. Robin Hanson invented LSMR and is also an advisor to Gnosis.

Augur was initially planning on using LMSR but decided against it. Augur claims that running LMSR on the Ethereum blockchain would be prohibitively expensive due to gas costs. LSMR requires many arithmetic operations. If a contract uses LSMR, every user would have to pay gas to execute the algorithm to purchase an outcome share. The fees could be high relative to the amount invested. We were not able to find commentary from Gnosis around how Gnosis plans to circumvent this challenge. More information about LSMR is available in the [LSMR paper](#).

Service Layer

This layer allows non-Gnosis entities to provide additional services on top of Gnosis Core. These entities can charge trading fees for the services they offer. Gnosis has discussed optimization tools such as chatbots, stablecoins, token wallets, and token exchanges - tools Gnosis believes developers will need to build consumer applications on Gnosis. Additional services can be added to this layer as needed.

Applications Layer

Gnosis aims to be a platform for third party developers to develop their own prediction market interfaces and develop dApps that pull data from Gnosis prediction markets. Gnosis Applications refers to applications built on top of the Gnosis platform by Gnosis or third party developers that integrate information from prediction markets. Gnosis provides developers with the basic development tools they would need to build such applications.

Gnosis is also conducting a contest, [Gnosis X](#), to encourage developers to build prediction market applications on Gnosis. Development teams can submit their ideas for a specific category and a winner is chosen per category. Winners are rewarded up to \$100,000 in GNO tokens to build the dApps. The current categories are Science and R&D, token diligence, and blockchain project integration.

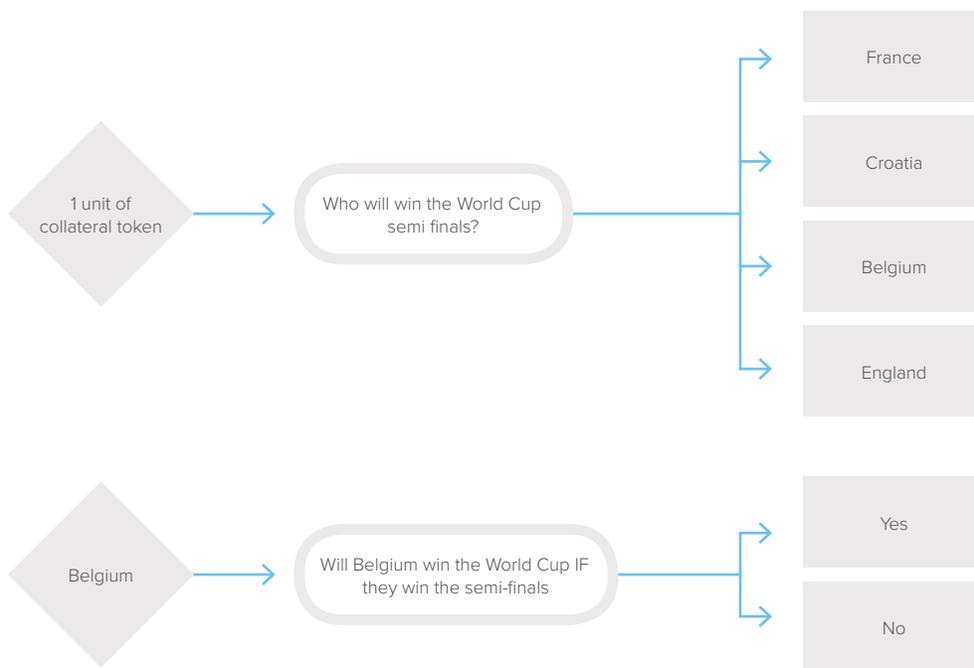
GNOSIS PREDICTION MARKET

Gnosis allows participants to create prediction markets on any event in any category. Prediction markets have at least two outcomes. They can be categorical (who will win the World Cup?) or scalar (What will the price of FB be on December 31, 2018?). Categorical markets can have multiple outcomes. Using the World Cup example, choices could be a) France b) England c) Germany d) Argentina e) Brazil, etc. Scalar markets have two outcomes - long (the price will rise) and short (the price will fall).

In Gnosis, participants buy a complete set of outcome tokens using collateral tokens (i.e. ETH). They pay a fee for converting collateral tokens to outcome tokens. It is not clear who fees are distributed to, but [this blog post](#) by Gnosis suggest that fees will be allocated to stakeholders in differing quantities. After acquiring the complete set, they can sell the token(s) associated with outcomes that they believe have a lower/no probability of occurring. Consider the market “Who will win the World Cup?”. There are four potential outcomes - Croatia, France, England, and Argentina. A user participates by buying \$100 worth of outcome shares. In return, the user receives 100 shares of Croatia, 100 shares of France, 100 shares of England, and 100 shares of Argentina. If the user believes that Croatia will win, the user can sell her shares of France, England, and Argentina at the current market price.

Once these tokens are on the market, users can directly purchase the token that corresponds to their belief. The price at which a particular outcome trades corresponds to the market’s expected probability that it occurs and aggregates the probability estimate of each participant. If the share of outcome A is trading at \$0.60, the market believes there’s a 60% chance that outcome A will occur.

Shares of outcomes are ERC-20 compatible tokens and can be used as collateral for further markets. Thus, Gnosis prediction markets could also capture conditional estimates. Some examples include the chance of a country’s GDP increasing if it leaves the European Union, the chance of a health care system reform given that a particular presidential candidate is elected, or the stock price of a company given that the current CEO is fired.



Source: medium.com/@akhounov

When the prediction market closes, an oracle chosen by the market creator reports on the outcome to resolve the market. Gnosis plans on offering an oracle marketplace, allowing market creators to designate an oracle of their choosing. Participants who hold shares of the winning payout win \$1 per share. Participants who hold shares of the losing outcome(s) don’t win anything.

Gnosis oracle⁸

Gnosis plans on providing centralized and decentralized oracles (aka the “Ultimate Oracle”). As it stands, It appears that the platform will rely on centralized oracles. Centralized oracles refer to providers such as [RealityKeys](#) and [Oracize](#). RealityKeys provides automated and human-verified data designed to enable automated information services. Oracize gives smart contracts the ability to access data they need from the internet in a trustless manner. Further down the line, Gnosis believes the platform can integrate centralized

⁸ forum.gnosis.pm/t/the-ultimate-oracle/61

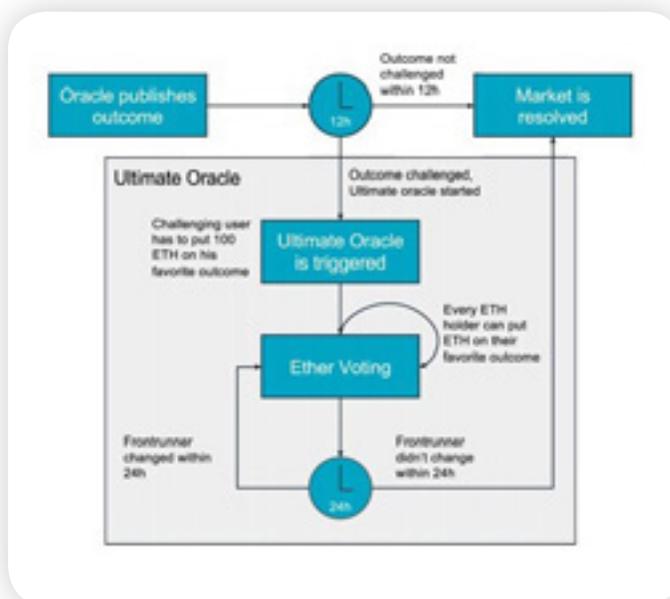
medium.com/@Cryptokeeper/the-gnosis-oracle-system-1cf8b8956950

providers like Wolfram Alpha and Bloomberg. Eventually, Gnosis plans on offering an Oracle marketplace to its third party developers and market creators.

Oracle Security. According to [Matt Liston](#), Gnosis would like to implement oracle reputations. Initially, social media reputation could serve as a proxy for determining the trustworthiness of an oracle. As the platform grows, Gnosis aims to have an internal reputation system whereby reputation is based on whether oracles have reported correctly on a consistent basis, whether the outcomes have been disputed, and so on. Matt also mentions that oracles can be required to post security deposits, which they would lose in the case of a dispute to provide an additional incentive (financial loss) to motivate them to report correctly. Gnosis could also implement a redundant oracle. This would require that multiple oracles report on a prediction market, making users more comfortable if all oracles report the same outcome. Unless there is randomization in choosing these oracles and a large enough set of oracles to choose from, there is always the risk of collusion. If users become an oracle the outcome reported is incorrect, they use what Gnosis calls the Ultimate Oracle to challenge the outcome.

Ultimate Oracle. The Ultimate Oracle refers to all ETH holders. The Ultimate Oracle kicks in if someone believes that the outcome reported by the centralized oracle is incorrect. In order to activate the ultimate oracle, a participant must post 100 ETH to dispute the reported outcome within 12 hours of reporting. This triggers “Ether voting”, which allows anyone to stake ETH on the outcome they believe is correct. An outcome is finalized when it has more ETH staked on it than any other outcome consistently for 24 hours. If the leading outcome changes within the 24-hour period, the clock is reset for another 24-hours.

The challenge with this backstop is that it is naive to assume that every ETH holder or even some ETH holders will take action and pay attention to or care about each and every prediction market created. In addition, the amount of ETH that must be staked is very high (100 ETH is worth \$21,000 at the time of writing). It is unclear if this amount must be staked by a single individual or entity or if multiple parties can contribute. If the answer is the former, then the individual may not have the funds to dispute the outcome or may not have enough skin in the game to care.



DUTCHX

DutchX is Gnosis' decentralized exchange for ERC-20 tokens based on the Dutch auction mechanism. During a Dutch auction, the price falls from an initial level as buyers submit bids at the price that corresponds with their highest willingness to pay. At auction close, all buyers pay the same price - the lowest price. This price is

at or lower than the price at which they bid. Gnosis highlights its reasoning for using the decentralized Dutch auction concept as follows:

1. Centralized exchanges have a high risk of loss of funds.
2. Exchanges face challenges around markets with low liquidity.
3. Using a Dutch auction protects buyers and sellers from causing large price movements with large orders.
4. Using a Dutch auction is more effective at preventing front-running associated with decentralized markets.
5. Using a Dutch auction allows the market to find a fair price for tokens. This is especially useful for illiquid tokens.

A key challenge with the auction model is that trades are not immediate and users cannot withdraw funds instantly. This makes fast trading impossible. Gnosis plans to facilitate trade of the outcome tokens created on Gnosis prediction markets on DutchX.

Sellers deposit their tokens before an auction starts. They cannot submit tokens into an active auction. If they deposit tokens after an auction has started, these tokens will be placed into the next auction. During an active auction, buyers submit their bids until the auction closes.

An auction in a certain token pair only starts if sellers have deposited a minimum of \$1,000 worth of tokens. In DutchX, subsequent auctions in the same token pairing are initially set at twice the final closing price of the prior auction. Once the auction starts, the price falls as buyers submit their bids. The auction closes when the price clears the quantity of tokens being bought and sold. At the close, all buyers pay the same closing price for their tokens.

Users do not need to own GNO or OWL to use DutchX, though they can use OWL to pay up to half of the platform fees. As a reminder, 1 OWL token is expected to be worth 1 USD. OWL tokens are burned upon use. Gnosis introduced the Magnolia (MGN) token to the DutchX platform in January 2018. MGN tokens are inflationary⁹. Participants do not need to own MGN in order to use the exchange. Rather MGN tokens are used as a reward to early users (buyers and sellers) to lower their platform fees. The more MGN a user holds as a percent of the total, the more the fee (currently 0.5%) is reduced. Gnosis generates and automatically credits 1 MGN to users for trading 1 ETH worth of any token. MGN does not have any function beyond lowering a participant's platform fees. To maintain the same level of fee reduction, participants have to be frequent users or buy unlocked MGN that other users are selling because MGN distribution is inflationary. Users can also buy more unlocked MGN to get to the next level of fee reduction.

TOKEN FUNCTION

Gnosis employs a complex three token model. GNO tokens generate OWL tokens, which are used as payment tokens to pay trading fees in Gnosis prediction markets. OWL tokens can also be used to pay fees in DutchX, which has its own native token called Magnolia (MGN) - we go over MGN in the DutchX section above.

GNO. The tokens that Gnosis offered during the token sale were GNO tokens. All GNO tokens were created at once. The supply is fixed to 10 million GNO. Users can buy and sell GNO on exchanges. The sole function of the GNO token is to generate OWL tokens. The OWL token gives GNO its utility.

OWL. OWL tokens (formerly called WIZ) serve the purpose of paying platform fees. Participants need to pay fees for generating outcome tokens. This is the only fee participants must pay for using Gnosis Core. OWL tokens are structured such that one OWL token pays for the equivalent of \$1 in fees. This is Gnosis' suggested method for paying fees, though participants can also pay fees in the collateral token in which a prediction market is denominated (i.e. ETH).

OWL tokens are generated by locking GNO tokens in a smart contract. There is no limit to the amount of GNO tokens that can be locked up. Users specify the lock period. OWL tokens are created algorithmically based on this lock period and the number of OWL tokens in circulation at that point in time. The OWL token

⁹ MGN are automatically locked upon dispersion. They can be unlocked but must remain locked for serving their function to lower fees.

supply at any given time is targeted to be 20 times the 3-month average monthly use of OWL. Gnosis says that OWL token issuance tracks actual usage to ensure that the value remains stable (1 OWL equals \$1). Users can see exactly how many OWL they will receive before locking up the desired amount of GNO tokens. Users will receive 30% of their designated OWL tokens upfront and the remaining 70% over the course of the GNO token lock-up period. Fees paid in OWL tokens are burned.

Users can also pay fees in collateral tokens. These collateral tokens are converted into GNO, which are then used in fee reduction mechanisms. Burning GNO or OWL means holding these tokens in a smart contract that cannot be accessed by anyone. Gnosis believes the majority of fees will be paid in OWL tokens because the price of OWL is pegged to \$1. Using collateral tokens such as ETH is risky due to the volatility of ETH and other crypto assets. Thus, if participants use collateral tokens such as ETH, they are not only betting on the outcome but also on the price of ETH. OWL tokens can also be transferred among users, though it is unlikely that they are used for speculative purposes because their supply is not fixed so their value can remain at \$1.



Collateral tokens. In Gnosis jargon, collateral tokens refer to the token in which a prediction market is denominated. According to the website, any ERC-20 token can be used as a collateral token. Participants turn collateral tokens into outcome tokens to participate in a prediction market. Participants have to pay fees for this conversation (0.5% of collateral deposited). They can pay these fees in collateral tokens or OWL tokens (theoretically worth \$1).

Outcome tokens. Every event outcome corresponds to an ERC-20 compatible outcome token. That means that every event contract will have at least two outcome tokens. Participants can store outcome tokens on the Gnosis Safe wallet and trade them on DutchX.

FUTARCHY

Gnosis is exploring Futarchy in the context of DAOs. DAOs are supposed to be automated. Gnosis claims that implementing Futarchy could result in automation of the entire governance process. Prediction markets would determine the best decision and smart contracts plugging into the market outcomes would automatically implement those decisions.

In March 2016, Gnosis received a developer grant from the Ethereum Foundation to conduct research on the decentralized Futarchy governance model. In 2Q18, Gnosis partnered with Robin Hanson to conduct cryptoeconomic experiments on the risks associated with Futarchy. This governance model is still undergoing research and is likely a long way from being implemented in practice. Read more about Gnosis' experiments with [Futarchy here](#).

GNOSIS-SPECIFIC CHALLENGES

Confusing token system

The Gnosis prediction markets platform uses two sets of tokens - GNO and OWL. GNO has no utility beyond generating OWL tokens. The steps are as follows: 1) users convert their fiat to ETH or BTC, 2) users buy GNO tokens with this ETH or BTC, 3) users lock up their GNO tokens in a smart contract, 4) users receive a portion of their OWL tokens upfront (30%) and the remainder (70%) over the period of the lock up. Users that generate too many OWL tokens can sell them to users who need OWL tokens. Alternatively, users can pay trading fees in the collateral token that the market is denominated in. Gnosis anticipates that the majority of users will use the GNO-OWL method rather than pay in the currency they're trading in and have the transaction cost slightly more. However, this method is not intuitive for users and requires a complex multi-step process just to pay trading fees on the platform. As the platform is still in beta, it remains to be seen what the preferred way to pay fees will be.

Ultimate Oracle

It seems that Gnosis plans to use centralized oracles to resolve most markets and use a decentralized oracle (the "Ultimate Oracle", aka ETH holders) as a backstop in the case of a dispute. However, skeptics argue that most participants won't have the funds or be willing to stake 100 ETH (about \$20,000) to kick off the Ultimate Oracle and most ETH holders won't be bothered to chime in and stake their ETH to resolve markets they don't care about. If the decentralized component of the Gnosis platform is useless, this begs the question, why go through the trouble of using a non-intuitive decentralized network, if users don't reap the benefits of decentralization?

Now let's say that some portion of ETH holders actually choose to chime in if an Ultimate Oracle is activated. The Ultimate Oracle would succeed in resolving the market correctly if participants stake ETH simultaneously, and if the amount of ETH staked on each outcome is hidden until the 24-hour window closes and the correct outcome is determined. In this case, participants are more likely to make an honest and straightforward choice and are less likely to be influenced by how much ETH is staked on each outcome. In Gnosis, however, the amount of ETH staked on each outcome is visible to all participants from the time the oracle is activated. Thus, if a participant sees that significantly more ETH is staked on the wrong outcome than the right outcome, she could refrain from staking ETH on either outcome or stake ETH on the wrong outcome because it is evident that outcome will win. Martin Koeppelmann's counterargument is that there will always be truthful actors willing to step in and counter balance a bad actor.

Finally, Gnosis has mentioned Ultimate Oracles could facilitate an Ethereum hard fork. Skeptics are dubious that ETH holders would risk a potential hard fork for a single dApp on the Ethereum network.

Ambiguous Timeline and Low Usage

Gnosis has been working on Gnosis prediction markets since 2015. Martin Koeppelmann said in 2017 that Gnosis is months away from launch and will beat Augur to market. Gnosis launched the Gnosis Trading Interface Beta on the Ethereum mainnet at the end of 2017. However, it is unclear if this is the final product, as it has "Beta" in the name and currently only has one open market. Gnosis also launched Gnosis Olympia at the end of 2017, which is a prediction market "tournament", or simply a simulation of its prediction market platform. Olympia is a dApp running on the Rinkeby network (Ethereum testnet). Gnosis held the first alpha test tournament for Olympia for two weeks starting December 2017, and ran 22 prediction markets. It held the second tournament during Dappcon (July 19-20) exclusively for Dappcon ticket holders. Augur, on the other hand, went live with a full working product on July 9, 2018. It currently has 1,447 markets and 96 liquid markets open on the platform.

Stox (STX)

OVERVIEW

Stox is a prediction markets platform built on Ethereum. Its native token is STX, an ERC-20 token. Unlike Augur and Gnosis, Stox employs a single token model. STX is used to pay fees, post collateral, and serves as the currency used for wagering. Stox was launched by the team behind invest.com. Invest.com is a digital trading and investment platform. The founding team consisted of nineteen members and six advisors.

On Stox, individuals can buy and sell outcome shares from event operators based on what they see as the probability at that given moment. While a market is active and trading, the price of outcome shares continue to fluctuate and indicate the probability of that outcome according to the participants.

Stox only allows trading outcomes of events that have a discrete number of potential outcomes. In other words, markets must be binary or categorical and cannot be scalar or continuous. If an event operator wants to create a market with inherently continuous outcomes (i.e. What will be the opening weekend box office revenue for the new Star Wars movie?), it must convert it into discrete outcomes that provide a range per outcome. Each event must also have a clear and well defined resolution point or time.

Two parties are required to facilitate trading in prediction markets - event providers and event operators. However, they are not always mutually exclusive. An entity can serve as both a provider and an operator. Alternatively, an event provider can select events created by different operators and offer users the ability to participate through the Stox app or another white-labeled app they might build.

Event providers provide users with access to the network via the original Stox app or via a branded/white-labeled version of the app using the reference implementation Stox makes available. Event providers in the Stox network also serve the function of promoting the platform to their users to drive traffic. Event providers earn syndication fees, which are a portion of the participation fee designated by an event operator.

Event operators (1) create events (2) serve as a centralized oracle, and (3) provide liquidity by serving as market maker. Event operators designate a participation fee when they create an event. A portion of the participation fee is paid to the event provider (aka the syndication fee).

Token sale

Stox held its token sale in July 2017. Stox received a celebrity endorsement from Floyd Mayweather, the boxing champion, who promoted the ICO on [his instagram](#). The token sale was apparently inaccessible to US investors. It raised 148,000 ETH (or \$33 million) for 50% of total STX tokens. STX was sold at a constant price during the ICO.

The max supply is 57 million and there are currently about 43 million tokens in circulation. A portion of token supply (12.5%) was allocated to invest.com as founding member in over a 12-month vesting period. 10% was allocated to the Stox team and 27.5% was allocated to the for-profit company, Stox Ltd. to bring strategic partners like invest.com onto the network.

Risk-free mode

Three months after the token sale, Stox launched an alpha version of the platform. In February 2018, it launched the beta version of the platform called Sun Tzu, and is currently operating in a beta "risk free mode". All STX used to buy shares are returned to users when the market resolves. Users who predict correctly receive "ranking points" in a 1:1 ratio, which accrue during the Monthly Stox Cup (a monthly tournament operated by Stox) and determine your rank on the leaderboard for that Stox Cup. To win STX tokens in beta, users have to place within the top 150 positions on the leaderboard. Every month, the leaderboard resets to zero. Stox grants users 50 demo STX tokens when they open an account in the beta phase. Users can add additional real STX tokens they might own. Stox plans to eventually move to risk mode when it goes live on mainnet. Once live, users will win actual STX tokens for making

a correct prediction and lose STX tokens for making an incorrect prediction. Below, we highlight aspects of the platform once it goes live.

What's next?

In terms of next steps, Stox plans on developing the Stox platform and app (including a mobile app), integrating with invest.com to bootstrap activity through its existing customers and providing potential partners with an SDK to build their own apps using the Stox back-end.

STOX PREDICTION MARKET

Event creation

While anyone, including individual users, can create an event and serve as event operator, Stox believes that the majority of events will be created by providers or larger entities and that different providers will focus on different niches (i.e. subsectors of sports, politics, financial markets, weather, etc.).

An event creator needs to specify certain parameters in order to create a market. These include:

- **Prediction Market:** Prediction market description or question
- **Potential outcomes:** Event operators must specify all potential discrete outcomes associated with any given event. After they create a market, participants can buy shares of what they believe will be the winning outcome.
- **Oracle:** the oracle is a source, process, or entity that the event operator will use to report the final outcome at resolution point.
- **Participation fee:** the participation fee is defined as a percent of the amount invested by a user in an outcome. A portion of the participation fee can be paid to event providers that are bringing traffic to the market by including the market in their application.
- **Syndication fee:** The event creator/operator also chooses the size of the syndication fee. For example, the event creator can specify a 1% participation fee of which 20% is designated for event providers that bring traffic.
- **Collateral:** event operators are required to post collateral in STX tokens when they create an event. The reason for doing this is to deter false reporting. The collateral must exceed a certain threshold of total investment in a given market. The collateral is locked up for 24-hours following the resolution point, during which time any user can dispute the reported outcome. If the dispute wins, the event operator who falsely reported the outcome will lose a portion of the collateral equivalent to the total amount placed on the "false" outcome. This amount will be distributed to participants who falsely lost.
- **Market maker reserve:** Event operators act as a market maker for their prediction market by providing initial liquidity. In order to do so, they must hold a reserve of STX tokens.

Event participation

Participants who want to buy shares of an outcome must specify the amount of STX tokens they want to spend, the outcome they want to buy, the provider (if they found the market on a provider app), and an optional limit price (the max amount they'd like to spend). The tokens are locked up until the event resolves. If the event resolves in their favor, they get back their investment and their proportion of the investment from the losing side(s). If theirs is a wrong outcome, they lose their investment. While the market is still live, they also have the option of selling their outcome shares if they want to exit their position before it resolves.

The price of outcome shares fluctuates as the level of activity changes. Stox plans to use a variant of the LSMR market maker algorithm to determine the market price. As we discuss in the Gnosis section, LSMR takes the total amount of tokens staked on each outcome into account when calculating the price. The price varies based on the supply and demand of outcome shares. The greater the volume and liquidity on a market, the larger trade volumes would have to be in order to cause a large shift in the price of shares. Augur decided against employing LSMR

because running LMSR on the Ethereum blockchain could be prohibitively expensive due to gas costs. If a contract uses LSMR, every user would have to pay gas to execute the algorithm to purchase an outcome share. The fees could be high relative to the amount invested. We were not able to find commentary from Gnosis or Stox around how they plan to address this challenge. More information about LSMR is available in the [LSMR paper](#).

Participants can discover events in which they want to trade via the Stox app(s). Providers that join the platform and curate apps for participants are incentivized to include markets created by other providers via the syndication fee. If a user finds another provider's market on their app, they receive a portion of the participation fee as designated by that event operator.

Stox oracle

As we mentioned, blockchains currently do not have a way to access real world data. Thus, dApps often need to rely on outside sources to report real world happenings to the blockchain. Stox uses a centralized oracle with a decentralized dispute mechanism rather than using a fully decentralized oracle to avoid slow convergence and resolution times.

Stox outlines two potential dispute mechanisms. The first method is to use the consensus of the network. In this method, the disputing party stakes tokens on the outcome they believe is correct. If the outcome has a majority of tokens staked for 24 hours, it becomes the winning outcome. The token holders who staked tokens on the winning outcome receive their staked tokens back and a proportional share of tokens from the losing side. The token holders who staked tokens on the losing outcome lose their tokens.

In the second method, Stox could poll a set of randomly chosen users about the correct outcome of an event in which a dispute is raised. Stox could incentivize these randomly chosen users by compensating them in funds from the collateral (if the dispute wins) or from funds staked by the disputing party (if the dispute loses).

Bancor integration

Stox uses the Bancor protocol to address the liquidity problem. The Bancor protocol provides continuous liquidity by using an on-chain automated market maker. Bancor allows users to convert between different ERC-20 tokens without going through an exchange. The Bancor smart contract will hold reserves of BNT (its native token) such that the BNT reserve in the contract is maintained at 4% of the total STX market cap. The primary reason for using this mechanism is to ensure that trades for STX tokens can always be filled. A secondary reason that Stox highlights is that because STX is backed by a BNT reserve, token holders can be assured that STX has intrinsic value. This is debatable.

The reserve is only set at 4% of the total STX market cap and it is unclear if this level is sufficient for ensuring that the token has intrinsic value. Further, BNT, the collateral token, is also a relatively new token and is similarly volatile – at this time, it is also correlated with the greater crypto asset market. It is possible that a market event not specific to BNT could still drive down the value of the BNT token and make it impossible to maintain the 4% reserve. Users can buy the tokens for use on the Stox platform directly from BNT smart token using Ether.

Sponsored ICO prediction markets

Stox has partnered with token projects who [sponsor prediction markets](#) around their token sale. Users who make correct predictions could win STX tokens and other tokens (of the token project sponsoring the market) from the prize pool. To date, Stox has held about 150 sponsored ICO prediction markets with about 50 token projects. The reason is to increase engagement on the Stox platform and increase awareness of and interest in ICOs.

TOKEN FUNCTION

The STX token serves two key functions:

1. Transaction fees, syndicate payments, oracle payments
2. Denomination currency of prediction markets

Users are required to purchase event outcomes in STX tokens. Users must also pay fees to event creators and market makers in STX tokens. Event operators must maintain collateral in STX tokens for the events they create and maintain a reserve of STX tokens to act as a counterparty or market maker in the events they create.

Stox Ltd

Stox Ltd is incorporated as a for-profit company in Gibraltar. It will derive revenues from providing “consulting services to companies using the Stox platform and its assets”. Stox Ltd has assumed the responsibility of (1) developing the smart contracts that power the Stox prediction market, (2) developing the Stox app (aka the original UI for the prediction markets platform), and (3) promoting Stox and bootstrapping activity on the platform. Stox Ltd does not serve as an event operator.

Stox has sixteen members. Yossi Perez, formerly the COO of invest.com, is the CEO of Stox. Ophir Gertner, the CEO of invest.com, is the founder of Stox and now an advisor to the company.

invest.com

invest.com is an online financial company which has been operating in the investment field since 2014. invest.com has over 3 million registered users and facilitated over 8 million transactions in 2016. invest.com allows users to actively manage their finances with stocks, indices, commodities, currencies, and other financial instruments and automated investment strategies. invest.com employs over 200 people across five cities (Berlin, London, Tel Aviv, Sofia, and Limassol). It has experience with regulators on online trading and is licensed to provide cross border investment services in the EU.

invest.com has multiple investment options for investors with different levels of experience. It offers regular trading, leveraged trading, social trading (similar to eToro). Invest.com also offers automated investment strategies to its users through robo-advisor technology.

Invest.com is serving as the Stox platform’s launch partner. As a launch partner, invest.com will develop an app and provide and operate events on the platform. Stox also plans to bootstrap activity on the platform by using invest.com’s existing user base. They plan to do so by opening a crypto wallet for each registered invest.com user. Stox believes that more incumbents will partner with Stox in similar ways to serve as event providers (and/or creators) as the platform grows. It plans to use a portion of funds from the ICO to act on this strategy.

Stox-specific challenges

Centralization. A challenge unique to Stox is its degree of centralization. Although Stox allows any user to create a prediction market, its strategy is to attract centralized “providers” (like invest.com) to operate prediction market apps and events because it claims that creating and operating prediction markets is an intensive task. This would turn Stox into a consortium of centralized “providers” offering prediction markets.

Additionally, although Stox will have a dispute mechanism in place when it launches on mainnet, providers and event operators could override disputes raised and sway the result in their favor given they are large entities that will likely have large reserves of STX tokens.

Further, having a consortium of centralized providers means that Stox is not technically censorship resistant. For example, if invest.com or other incumbent creates or incorporates a prediction market that regulators dislike, they can tell invest.com to take it down or take regulatory action against them.

Sponsored ICO prediction markets. Stox has been partnering with token projects prior to their ICO in order to entice users to predict aspects of the ICO, driving volume to its platform, and increase awareness of the ICO to attract more investors to the ICO. This seems like murky regulatory territory given the commentary from different regulators globally around all ICOs being securities.

Celebrity endorsement. Stox received a celebrity endorsement from Floyd Mayweather. In general, ICOs endorsed by celebrities who in reality know very little about the project or ecosystem have turned out to be fraudulent or scams. While Stox does not appear to be a scam thus far, there is negative press associated with celebrity endorsements.

GENERAL PM CHALLENGES

Platform risk

Current prediction markets (Gnosis, Augur, Stox) are built on Ethereum. Thus, they can only be as scalable as the platform they build upon. Ethereum's throughput is still very low (~7 tps for ERC-20 tokens). At the time of writing, there were over 81,500 pending transactions on Etherscan. Although Ethereum is working on scaling solutions to increase throughput, it remains to be seen when the solutions will actually be implemented. The dApps' ability to scale and draw users is contingent on Ethereum's timeline and ability to scale.

Further, outcome share prices can be gamed due to Ethereum's network delay. Someone can manipulate share prices by flooding the network with high sell offers with high gas prices, that would crowd lower-priced sell offers and result in an inaccurate share price.

Ethereum also faces competition from additional smart contract platforms building in scalability from the ground up (i.e. EOS, Cardano, Dfinity, etc.). If these platforms prove to be as secure (if not more) and more scalable than Ethereum, these dApps could face competition from prediction markets that build on these platforms, if they don't port over to one of the new, more scalable platforms.

Competition

Augur, Gnosis, and Stox face competition from each other and centralized platforms (PredictIt, Betfair, Fairplay, etc.). At this point in time, Augur's prediction market platform is being more heavily used than Gnosis and Stox. If prediction market participants believe that Augur is more intuitive and more decentralized, it will be difficult to take share from Augur.

Gnosis is differentiated from Augur and Stox in that it offers additional products and services such as DutchX, Gnosis Safe, Gnosis Apollo, etc., though we do not know how heavily these products and services are being and will be used.

Stox differs from Gnosis and Augur in its strategy of using centralized "providers" to bootstrap activity. To the extent this strategy works, it could gain and retain more users more quickly and effectively. However, this strategy could also deter crypto users as it is more centralized than Gnosis and Augur.

Regulation

Although the respective project teams claim they are not in violation of any laws because it is not creating markets (the users are), there is still the risk of regulators seizing funds and shutting down the web interface if they rule that developers are in violation of any laws. On the flipside, because these markets are decentralized, technically any developer team can build a new web interface if the current interface is shut down.

Due to its decentralized nature, these markets do present a challenge to regulators. The trading activity is similar to gambling and options trading in traditional financial markets. Currently, options trading is part of a strictly regulated global financial derivatives market that is only accessible to a limited number of accredited and experienced investors. Decentralized prediction markets open up this market to any participant, experienced or not. If they are used to create options trading type markets, the CFTC and other regulators globally have little ability to take legal action due to the decentralized and global nature of the platform. Further, once the mainnet is live, the platforms are no longer in the control of the founders. They have no power to shut down the network, even if regulators confiscate funds and shut down the web UI.

Recently, a CFTC commissioner (Brian Quintenz) made comments about prediction markets in his speech at the 38th annual GITEX Technology Week Conference. He said that "the CFTC has determined that the smart contracts executed on the blockchain are binary options, which are within the CFTC's jurisdiction. Binary options are a type of option whose payoff is either a fixed amount or zero. For example, there could be a binary option that pays \$100 if the price of gold is above \$1,200 per ounce on a specified date and zero otherwise." Further, he said markets created around "war, terrorism, assassination, or other similar incidents" fall under the CFTC's purview because if enacted, they are against the law. He went on to say that in the past, the CFTC has only allowed prediction markets in limited circumstances on specific events or for academic purposes and has restricted retail investor access.

Regulation on prediction markets or its developers would be detrimental to the success of these platforms. However, at this time, it is unclear whether the CFTC will heed these recommendations and if it does, *how* it plans to enforce regulations against decentralized prediction markets, given there is no central point of attack.

Fees

Although the fees market creators and reporters collect are low (1-2%), there are layers of fees users must pay to use the platforms and these fees add up. In Augur, from lowest to highest, these include reporting fees (0.01%), market creator fees (1-2%), Ethereum gas fees (depends on the size of order), and fees for converting fiat to ETH (4% on Coinbase if using debit/1.5% if using ACH). Thus, total fees for trading on Augur range from 3.5% to 9% or more. Participants on Gnosis and Stox also have to assume gas fees and conversion fees (fiat to ETH to native token). On Gnosis, participants trading outcomes have to pay a 0.5% fee to the market creator. On Stox, the event creator sets the participation fee, but the exact percentage is unclear and can vary. High fees are contrary to the idea that decentralized prediction markets are more accessible because they are cheaper.

Malicious markets

Decentralized prediction markets have no restriction or censorship on the kinds of markets that can be created. As a result, there is nothing preventing participants from creating malicious markets, on topics like assassinations and terrorist events. In such markets, malicious actors who buy “yes” shares are incentivized to carry out that act to make a profit.

Parasitic markets.

Parasitic markets are markets that use the result of the oracle without paying fees. A prediction market that is issuing bets on well known events will likely have competition from markets betting on the same event and there is the risk that this market will reuse the results without paying appropriate reporting fees.

Low liquidity

Decentralized prediction markets are still fairly new and many markets do not have sufficient liquidity, in terms of the number of shares traded of each outcome, to attract token holders onto the platform. Users may not have confidence that they will get shares of any outcome at a price they are comfortable with. They may also worry that there won't be sufficient liquidity to fill their order if they need to exit their position and settle the market contract. To solve for this, Augur and Stox suggest that market creators also serve as market makers to bootstrap liquidity in their markets. There is little information on how Gnosis has been addressing this challenge.

CONCLUSION

Of the three projects, Augur currently has the most users and activity. It experienced a surge in bets during the 2018 midterm elections, surpassing \$1.5 million. The platform reached an all time high in volume on 11/7, at 2935 ETH, according to DappRadar, though the volume dropped to 250 ETH on 11/8. DappRadar does not have data on the volume on Stox and Gnosis. According to State of the Dapps, Augur has 66 daily active users and Stox has 44 daily active users. State of the Dapps does not have data on the daily active users on Gnosis.

While these projects have users, the concept of prediction markets and dApps are foreign to the general public. Further, the barrier to entry for using dApps for regular users who aren't immersed in the crypto and the blockchain world is steep. An increase in adoption will require a significant improvement in scalability and design and UI that manages to hide some of the complexity and a simplification of fees and processes that make it less confusing and challenging and more intuitive and enjoyable for users to participate.

Until dApp developers can get their applications to a point where they look and feel like (or better than) their centralized counterparts (even going as far as hiding the fact that these applications run on a blockchain), users stand to benefit from step-by-step guides educating those who have no experience or knowledge about crypto and blockchains on the components and processes of the platform.

Further, prediction markets are a relatively new tool for finding answers and aggregating information. Such markets are not as familiar or understood to the same extent as polls and surveys and it is still unclear if and how these markets will be regulated. While blockchain technology offers unique opportunities for perfecting prediction markets through incentivizing participation and decentralizing reporting, optimizing this tool and increasing adoption will likely require experimentation, iterations, adjustments and more regulatory clarity.

Product/Service	Augur	Gnosis	Stox	Bitcoin	Ethereum
Github commits	28.8k	0.48k	0.07k	18.7k	10.2k
Github contributors	57	10	1	584	351
Twitter followers	121k	71.6k	14.5k	917k	434k
Reddit followers	9.5k	2.2k	2.2k	980k	402k
Open Markets	1,447	3	54	N/A	N/A
Liquid Markets	96	0	N/A	N/A	N/A
Token Sale	\$5.5m	\$12.5m	\$33m	N/A	\$18m

