PredictX

April 24, 2021

1 Introduction

Prediction markets are online platforms where individuals can set a price on the realization of a future event. These markets encompass a wide range of activities and events from sports betting, politics, to price predictions on stocks like TSLA, and even other events like albums releases, IPO's, etc. The goal of prediction markets ultimately is to provide everyone with an accurate source of information, first and foremost. Those who forecast the outcome correctly win money in addition, and those who forecast incorrectly lose money. Existing prediction market platforms are highly centralized in the form of sportsbooks, online betting platforms and applications. However, there are several issues with centralized prediction markets like Betfair currently:

- The platform has control over user funds

- The platform charges 3-10% fees on users' transactions along with significant withdrawal fees or hurdles

- The resolution of markets is centralized and dependent on chosen sources of information

- Users have little to no control over the types of markets listed on the platform

- Market Makers can add or pull bids/asks constantly and change betting lines in order-book style markets

By decentralizing prediction markets, it is possible to solve all of the above except that of market makers pulling liquidity and changing betting lines. Over the past few years, several architectures have been proposed, with Augur pioneering the first order-book based decentralized prediction market and Gnosis attempting to expand Augur's offering with the introduction of an automated market maker provision.

Automated Market Makers work well for cases in which liquidity providers do not have to manage liquidity actively. In addition, AMMs are great for cases in which odds are not changing too rapidly second-to-second, although this can be dealt with too with more sensitive AMM curves.

2   Competitors

Despite the introduction of several decentralized prediction market protocols, users have not been able to have a seamless experience using them. The main competitors are:

- Augur - Order book based, has a decentralized resolution and dispute system

- Gnosis - Allows for a decentralized system with an automated market maker

- Omen - Using Gnosis as the backend protocol, offers a front-end that is easier to interact with

- Catnip - Using Augur as the backend protocol, offers a front-end that wraps Augur's ERC-1155 tokens as ERC-20 tokens (yes/no shares) and deposits them into a 3-sided Balancer Pool

- Polymarket - Using Gnosis as a backend, has the most user-friendly interface on the market currently and executes orders on a sidechain of ethereum (Matic)

2.1   Issues with Current Competitors

While the existing competitors have paved the path for a great product, they all suffer from specific issues:

- Augur - Poor UX, low liquidity, almost no volume, inflexible order-book model.

- Gnosis - Poor UX, low liquidity, almost no volume.

- Catnip - Better UX than Augur, but still has relatively poor UX to traditional fintech and betting products. Requires multiple steps to add liquidity.

- Polymarket - Much better UX than the other products but not fully decentralized wallet system, and has relatively low liquidity for some of the markets

In addition to the above, there are problems shared by all the platforms:

- Built on base-layer ethereum, struggle with high gas fees

- Even if moved to L2, struggle with the architectural limitations of the L2

- Lack token incentives for ensuring liquidity in markets

In order to address the above issues, PredictX aims to be the most user-friendly prediction markets platform powered by a truly decentralized protocol that can integrate with other DeFi platforms. This vision will take several phases to execute, starting with a deployment in Ethereum for v0.

3 PredictX Architecture and Trader Mechanics - v0

As Augur is based on an order-book model, it becomes difficult for the general user who simply wants to place a bet on a potential outcome, but instead has to worry about trade execution and price-points. The interface afforded by an automated market maker (AMM) allows users to buy with some slippage described by the interface and a single quoted price. In the case of AMMs, there is flexibility in what sort of curves are used for the AMMs. v0 of PredictX used an architecture similar to Catnip, where a market issued on Augur has ERC-1155 tokens to represent Yes/No Outcomes. These tokens are then wrapped into ERC-20 tokens and deposited into a Balancer Pool. The tokens are represented as Yes/No shares in the front-end for the user. The actions of buying shares, selling shares and adding liquidity are each governed by equations related to Balancer as well as to the specific mechanics of a specific prediction market platform.

The complexities of the balancer pool calculations can be simplified by considering a constant-product pool instead. The constant-product function is used in Uniswap and is enough to understand the basic mechanics of traders on the platform.

To circumvent this two-step and complex architecture, the PredictX v1 is under development and to go live soon.

4 PredictX Architecture and Trader Mechanics on Binance Smart Chain - v1

To provide a great user-experience, the PredictX project began deployment on Binance Smart Chain and a change in the architecture, while still utilizing automated market makers. The backend has shifted from the Augur+Balancer to a model based on Gnosis, which allows for more flexibility with the AMM curves. The combination of low-fees and low front-running possibilities due to the validator structure of Binance Smart Chain makes prediction markets usable by the general public, which was not possible before on Ethereum.

4.1 A short introduction to Conditional Tokens

The Gnosis framework is based on Conditional Tokens, which is an innovation that allows for the existence of Combinatorial Markets. A Conditional token, represented by the ERC-1155 token standard, allows us to represent complicated events such as: "Will Joe Biden win the election AND Tax on Capital gains not rise in 2021?" as tokens that resolve to a 0 or 1 price. The key sructure underlying these Conditional Tokens is a **Condition** with the following parameters:

- oracle – The account assigned to report the result for the prepared condition.

- questionId – An identifier for the question to be answered by the oracle.

- outcomeSlotCount – The number of outcome slots which should be used for this condition. Must not exceed 256.

With the above structure, we are able to map Conditions to token "outcomes" and hence offer markets. This now brings us to the actual implementation on BSC.

4.2 Implementation on Binance Smart Chain

Since Binance is EVM compatible, the integration with Binance Smart Chain requires only minor changes, but makes a huge difference to user experience and the possibilities of prediction markets. While the Omen project has implemented on XDai, we believe that BSC offers liquidity and defi-composability that is unparalleled. Below we describe the trader and LP mechanics in the case of a fixed-product market maker, which is what we begin with initially.

4.3 Trader Buys Shares

If y and n refer to the amounts of yes and no shares in a pool, respectively, then in the case of the constant product market maker the following equation holds:

$$\theta = y * n \tag{1}$$

Let us say a trader decides to buy yes shares with ϕ dollars.

- ϕ yes shares and ϕ no shares are minted

- After these shares are added to the pool, there are $(y + \phi)$ yes shares and $(n + \phi)$ no shares in the pool

- Then, the trader gets y_T yes shares back by transacting with the pool automatically such that the invariant is satisfied.

$$\theta = (y + \phi - y_T)(n + \phi) \tag{2}$$

We can solve for y_T to get:

$$y_T = \frac{\phi^2 + \phi(y + n) + y * n - \theta}{n + \phi} \tag{3}$$

If instead the trader wanted to buy a specific amount y_T yes shares, then the pool would change as:

$$\theta = (y + \psi - Y_T)(N + \psi) \tag{4}$$

Where ψ is the cost of buying the shares. This is an unknown variable. y_T is the number of yes shares the trader gets. This makes more sense from a user

perspective.

The equation can be rewritten as:

$$\psi^2 + (y + n - y_T) * \psi + (y * n - y_T n - \theta) = 0 \tag{5}$$

Solving the quadratic equation gives us a value for ψ.

Note that once we have ψ, we can compute the slippage as the ratio between ψ and the implied price of Y_T yes shares at spot price.

4.4   Selling Shares

Starting with the constant-product uniswap equation:

$$\theta = y * n \tag{6}$$

and a trader who sells y_T shares. Then, the new equation for the AMM becomes:

$$\theta = (y + y_{T*})(n - n_T) \tag{7}$$

as well as the condition:

$$y_T - y_{T*} = n_T \tag{8}$$

This condition means that an equal amount of yes and no shares that are "left" over are then burned. These conditions can be combined to give:

$$y_{T*}^2 + (y + n - y_T)y_{T*} - yy_T = 0 \tag{9}$$

Solving the equation, it is possible to derive y_{T*}. The amount that the trader gets is: $y_T - y_{T*}$ in the base currency (USD).

4.5   Adding & Removing Liquidity

When adding ψ worth of liquidity, ψ yes shares and ψ no shares are created and added to the pool. This changes the constant θ for the pool, and decreases slippage. Slippage is a strict function of liquiidty in the pool regardless of the AMM curves chosen and this is consistent across all platforms such as Balancer, Uniswap, Curve.

4.6   Incentivizing LPs

To keep track of how much liquidity is provided, a certain number of synthetic tokens - sPRED is given to the liquidity providers and is redeemed for the base currency (BUSD). This method is common in multiple LP situations for lending protocols as well as liquidity farms. On PredictX, Liquidity Providers gain significant rewards from the fees per trade as well as other potential benefits to be decided via governance.

On the PredictX platform, we will have a synthetic stablecoin pxUSD which will

be the base currency that traders receive in return for their trades. pxUSD will be 1:1 redeemable for BUSD (and other stablecoins that our platform decides to support).

The BUSD and other accepted stablecoins from LPs will be deposited in lending protocols and yield farms on Binance Smart Chain, hence yielding returns for LPs during the duration of the markets. When LPs decide to withdraw their liquidity by returning their sPRED, they get back the equivalent amount of BUSD from the pool as well as their split of the interest from lending/yield farms that PredictX integrates with (such as Nerve Finance).

4.7   Progressive Decentralization

While the market resolution will initially be decided by PredictX, with the iterated version of the platform, a governance mechanism will allow new resolvers to be decided so that event resolution can be staked for and decided upon by a group of resolvers. This way even resolution will be decentralized and rewards for providing accurate resolution will be split between the group of chosen resolvers.

5   Project Vision and Roadmap

The issues with Ethereum gas fees have forced many projects to build on layer 2 solutions as well as on other chains. Polymarket, a prediction market platform, processes all transcations on matic, a sidechain of Ethereum. Other projects are considering building on Arbitrum and Optimism. The issue with layer 2 solutions is the continued problem of exit games, possibly centralized control and any other issues with the base layer protocol.

In order to truly give a superior user experience and combat Ethereum gas fees for a DeFi protocol like PredictX, v1 of PredictX will be deployed on Binance Smart Chain (BSC) with later versions on Polkadot.

There are multiple benefits to building on Binance Smart Chain and Polkadot:

- Low gas fees, ease of usability

- Easy transition from Ethereum, as parachains of Polkadot such as MoonBeam support solidity/are EVM compatible.

- Building for a cross-chain world

- Inviting new users from other chains to participate in markets

The Roadmap of PredictX is broken down as follows:

- V0 launch: First market launched with AMM-based backend

- V0.1: More markets launching targeting multiple regions globally

- V1.0 Implement on Binance Smart Chain pending technical milestones

- V1.1 launch: Implementation of first AMM and different AMM curves on Moonbeam (an EVM compatible parachain)

- V1.2: Migration to Polkadot via Moonbeam

- V2 launch: Integration of DeFi protocols such as Compound and Yearn for LPs to allow additional passive yield generation

- V2.1: Adding cross-chain support for markets

- V3: Add Private Betting Pools and automatic market creation

- V4: Add voting system for new markets and improvement proposals (IPs). Add decentralized oracle resolution system (integration with Chainlink)

6 Conclusion

We see prediction markets as the first use case for DeFi that moves beyond financial use cases of lending, trading, farming etc and can become a mass product with millions of users. Our roadmap to V4 is just the beginning of the journey to develop our AMM-based platform into a platform for everyday users that can compete with its centralized counterparts. Our end goal is to create a user-friendly prediction markets platform powered by a truly decentralized protocol that is easily integrated with other DeFi platforms and other blockchains. This means non-custodial, not centralized and open to everyone.