

NEZHA.FI



NEZHA

THE LIQUIDITY ENGINE
FOR NEXT GENERATION PREDICTION MARKETS

WHITEPAPER V1.6
MARCH 2022



1. INTRODUCTION	P – 3
2. NEZHA DETAILS	P – 4
3. PROTOCOL MECHANISMS:	P – 5
PREDICTION POOL	P – 5
ROLLOVER POOL	P – 8
OPERATIONAL POOL	P – 8
RESERVE POOL	P – 8
AFFILIATE FLYWHEEL POOL	P – 9
NEZHA FOUNDATION POOL	P – 9
PLANNED DEVELOPMENTS OF THE NEZHA LIQUIDITY ENGINE	P – 10
ADDITIONAL PREDICTION MARKETS	P – 10
N PREDICTION POOLS	P – 11
ROLLOVER POOLS	P – 11
4. TOKENOMICS	P – 12
PREMIUM TIERS	P – 12
GOVERNANCE	P – 12
POOL ORIGINATION	P – 13
LIQUIDITY MINING	P – 13
BUYBACK AND BURN POOL	P – 13
TOKEN DISTRIBUTION	P – 14
5. LAUNCH PLANS	P – 16



1. INTRODUCTION

Records of prediction markets can be traced back as far as 1503, while some argue that they could be as old as humankind itself. They have stood the test of time, enriched cultures, and contributed to people's lives with thrill and joy throughout history. Lately, these markets have enjoyed increased popularity, with the number of market participants significantly increasing due to regulatory changes and the ease of online access. Still, this comes almost as a surprise, considering how little innovation prediction markets have experienced overall. Even though new games have been developed and the internet has enabled the birth of new entertainment sources, the binary result of financial gain or loss has persisted ever since. As such, new incremental innovations might have led to new sources of entertainment, but no disruptive changes have been introduced to capture greater value for the consumers in prediction markets. Traditionally, the chance for financial loss almost always trumped the chances of financial gain for the consumers, arguably reducing the long-term entertainment factor through the experienced loss. We don't believe that these dynamics are the final stage in the evolution of prediction markets.

This is where Nezha positions itself: Introducing the next generation of prediction markets.

Nezha is the liquidity engine for prediction markets where the participants do not wager the principal stake but rather the yield generated on the pooled principal of all participants. Through staking liquidity and yield aggregation, Nezha utilises the power of DeFi to change the old industry dynamics radically. These improvements have no adverse effect on the essential characteristic of first-generation prediction markets that we intend to maintain: the greatest entertainment. The next generation of prediction markets offers the same joy and incentive of financial gain without the looming risk of financial loss. Additionally, the next generation incentivises larger stakes, increased liquidity and positive flywheel effects for the prediction market distributors. Due to the positive-sum dynamics and positive expected outcomes for protocol participants, the next generation of prediction markets is a gamified staking strategy rather than only a source of entertainment. Through yield aggregation and game characteristics, protocol participants not only enjoy games but become eligible to win the accumulated YieldPot during each game cycle.

2. NEZHA DETAILS



Nezha plans to position itself as a leading gamified yield aggregator by offering positive-sum prediction markets. In doing so, we provide both a novel alternative to traditional DeFi yield strategies and change inherently zero-sum prediction games for the better.

Through staking stablecoins in the Nezha Protocol, DeFi stakers can maintain the benefits of stablecoins, while gaining exposure to the chance of high rewards through winning the Nezha prediction games instead of receiving continuous yield as being the benchmark state of other DeFi protocols. As such, the Nezha games enable chances for large multipliers while minimising downside risks, regardless if the market is trading sideways, down or up. The protocol offers an exciting new alternative to utilising stablecoin reserves instead of simply holding them or staking for guaranteed but modest APRs. Secondly, Nezha gives prediction market enthusiasts an attractive option to partake in prediction games while limiting risks through staking their principal stakes in yield routing contracts instead of wagering the principle itself. Instead of wagering stakes with the negative expected outcomes, Nezha pools liquidity and uses yield routing across DeFi protocols to distribute yield to prediction market participants.

To fulfil this mission, Nezha is developing an ecosystem with a multitude of mechanisms to ensure attractive yields, security, and long-term growth and stability. As the core of the ecosystem, Nezha's liquidity engine directs liquidity from prediction market participants into yield protocols. Sustainable liquidity flows are stimulated through the offering of a new area of prediction market entertainment, achieved through sophisticated game development, combined with quickly scaling attractive yield opportunities.

To gain access to the prediction games, users will be required to stake into the NEZ protocol, where their stake will remain locked until the end of each game's cycle. After the lockup period, participants can withdraw their principal stake and any gains or leave their balance staked to participate in the next game's cycle. The assets are pooled and routed to external yield producing protocols. These protocols will generate daily compounding yield that is distributed weekly into the Nezha pools.

3. PROTOCOL MECHANISMS



Each week, the accumulated returns from the yield protocols will be allocated to various pools. Each of the pools plays a vital role in the Nezha ecosystem. Details about each of the pools will be introduced in the following section.

PREDICTION POOL

Each week, the potential yield available for distribution among the winning participants is transferred to the prediction pool, which accounts for the majority of the generated weekly interest. Depending on the outcome of the weekly prediction game, the YieldPot is available to be claimed by the owners of the participating wallet addresses. The YieldPot is equal to one hundred per cent of the Prediction Pool in any given week. Depending on the prediction game mechanisms, winners will be determined based on the outcomes of each weekly game cycle. In the first iteration, Nezha will be launching a Prediction Draw Game in which six numbers are attributed to each entry in the prediction market. Each participant is awarded entries proportional to the number of tokens staked into the protocol. The entries hold the series of numbers as well as a unique identifying id per entry ticket.

Each series of numbers is generated through a True Randomness Generator using atmospheric noise to translate it into a sequence of random numbers. A separate sequence is initiated to generate the winning number of the lottery. Using a VRF infrastructure, we generate a sequence of 6 unique numbers generated at random using Goldberg's verifiable random function. In this function, a public and a secret key are generated. The secret key is generated by selecting a number from the secp245k1 elliptic curve used by Ethereum's cryptography. The contract request from Nezha creates a seed key while the Oracle creates a public key. Firstly using these two keys to hash the input to the curve, we obtain a cryptographically secure sample from secp245k1. This is assured through recursive hashing the inputs using keccak256 until the output is less than the order of secp256k1s base field ("p"). This is the x ordinate of a random point (x,y) on the secp245k1.

The ordinate is then multiplied as a secp256k1 curve point by the secret key to obtain point γ . The keccak256 hash of γ , as a uint256, is the VRF output. It generates proof that γ is the same multiple of (x,y) as the oracle's public key is of the secp256k1



generator. Then it computes $v=n \times (x,y)$. Next, it hashes together (x,y) , its VRF public key, γ , the address of u , and v , takes the remainder of that hash modulo $\#secp256k1$, and calls that c . Finally, it computes $s=n-c \times k$ modulo $\#secp256k1$, where k is its secret VRF key. The proof is its public key, γ , c , s , and its input seed. It sends this back to the on-chain VRF machinery, which verifies the proof, and sends the output back to the consuming contract, assuming the proof verifies. This assured true randomness as well as transparency for all market participants.

For the first game iteration, payouts from the prediction pool are structured into two tiers. In the event that any participant holds four or more of the drawn numbers in the correct order, they hold a claim to part of the Prediction Pool. All participants who hold four out of six drawn numbers in the correct order are awarded a claim of the total YieldPot. Market participants who hold five out of six numbers matching the prediction market outcome in the correct order will be awarded a higher claim of the total YieldPot. Market participants who hold six out of six numbers matching the prediction market outcome in the correct order will be awarded the grand prize. This grand prize is backed through an insurance payout. The grand prize will vary on a weekly basis and depends on the APY available and the TVL. Furthermore, to celebrate such an event, participants who hold six out of six will be awarded exclusively minted NFTs.

These dynamics provide sufficient variety to assure non-bias towards large market participants as well as continuous increases in value of the yield generating sum. The likelihood of the first five numbers being drawn is calculated as:

$$\frac{56!}{5!(56-5)!} = \frac{56 \times 55 \times 54 \times 53 \times 52 \times 51!}{5 \times 4 \times 3 \times 2 \times 1 \times 51!} = \frac{458.377.920}{120} = 3,819,816$$

In the first draw, five numbers are randomly drawn out of a sample of fifty-six where ! indicates $n! = n \times (n-1) \times (n-2) \times \dots \times 2 \times 1$

In the second tier of the draw one number is drawn from a sample of ten resulting in:

$$\frac{10!}{1!(10-1)!} = 10$$



As such follows that the chances of a top level draw are equal to:

$$\frac{1}{3,819,816} \times \frac{1}{10} = \frac{1}{3,819,8160}$$

The chance of a second level prize draw are hence equal to:

$$\frac{1}{3,819,816} \times \frac{9}{10} = \frac{1}{4244240}$$

The third and last tier with guaranteed access to the YieldPot hence follows the probability of:

$$\frac{255}{3,819,816} \times \frac{9}{10} = \frac{51}{848848}$$



ROLLOVER POOL

All yield that has not been distributed according to market outcomes will be automatically rolled over into the Rollover Pool. The Rollover Pool routes the assets back into yield generating opportunities. There, they continue to be compounded on a daily basis, generating further value for the next cycle's distribution and the Nezha ecosystem.

OPERATIONAL POOL

A percentage of the yield generated will be awarded into the Operational Fund Pool, which is crucial to sustaining the ongoing development of the Nezha ecosystem. The share required to fund operations will vary depending on the stage of development and market conditions. Therefore, rates might vary for the operational fund pool. Altogether, the pool will cover operating expenses such as payroll expenses, legal expenses, marketing costs, further technological developments, general and administrative expenses, or other operating expenses. The Operational Pool will be managed by the board and association members of the Nezha DAO.

RESERVE POOL

As protecting our community is of greatest priority for Nezha, it is crucial to implement mechanisms that protect our protocol participants against losses of their assets. To do so, Nezha is implementing risk hedges against risks such as smart contract risk as well as market participant defaults. A percentage of the yield generated each week will be dedicated to our own Reserve Pool. This Reserve Pool will be built up over time. Initially, this reserve pool will be subsidised by our native token NEZ but will shift to full stable coin based as liquidity in the protocol allows.



AFFILIATE FLYWHEEL POOL

A further part of the generated yield is routed to fund our affiliate flywheel pool. Assets in the pool will be paid out as rewards for referrals and shared among any people introducing new members to the Nezha ecosystem at any given time. Referral payouts will be made automatically as certain triggers are fulfilled. These include the participation in at least one full cycle of a Nezha game by the referred party. Payouts in the Affiliate Flywheel Pool will occur on a monthly basis and will be awarded pro-rata to the overall amount of referrals made. Depending on the current pool size, the flywheel pool may be subsidised with our native token NEZ to encourage the organic growth of the Nezha ecosystem at all times.

NEZAH FOUNDATION POOL

Furthermore, ten percent of the generated yield flows into our Nezha foundation pool. This pool will be created as soon as Nezha has reached operational sustainability. As Nezha is committed to empowering the individual through technological advancements, the foundation pool marks an important contribution to change the world for the better. In doing so, the foundation pool is using its capital to promote equal access to technology and fund access to computer science education, with the ambition to inspire positive change. Believing in the power of innovating within stagnant markets, it is our ambition to support individuals who seek to improve other industries and processes to disrupt the status quo. We aim to operate this initiative at a global scale, harnessing the potential in many of the regions with too little access to needed funding.



PLANNED DEVELOPMENTS OF THE NEZHA LIQUIDITY ENGINE

A second stage of the Nezha ecosystem will be introduced after sufficient scaling of the current operations. These developments will centre around adding further utilities for our token holders and to the ecosystem. Aside from the already implemented mechanisms, the following awaits to be added to the Nezha ecosystem:

ADDITIONAL PREDICTION MARKETS

First, a variety of new prediction market games are planned to be offered to the community. To encompass the organic development and implementation of such, different actors and mechanisms need to be introduced. With the core utility of the liquidity engine remaining unchanged, the yield will be distributed among the different prediction game pools. In doing so, Nezha will be offering a multitude of different prediction market games, growing an ecosystem of diverse entertainment options for our community. Next to the development of further internal games, Nezha will open the ecosystem to community-led development of games. Moreover, Nezha will make its technology accessible through white-labelling so other operations may offer non-Nezha branded prediction market games on their platform leveraging the technologies built by Nezha.



N PREDICTION POOLS

To achieve such, multiple prediction pools for each of the introduced prediction games are needed. The basic functionality of such pools remains the same: protocol participants can receive yield from the prediction pools distributed to them depending on the game's outcome. For all Prediction Pools relating to internal games published by Nezha, these will be done automatically, and their mechanics will be defined by the Nezha DAO consisting of its board and members. For the origination of Whitelabel prediction pools, the operator will receive the flexibility to change the distribution mechanics to their liking. Hence, Nezha will continue to manage liquidity for all Whitelabel solutions; however, the operator will be responsible for the organisation of governance of the distribution mechanics. For all community lead new game proposals, the community member will need to stake a certain amount of NEZ to be able to originate a new Prediction Pool. The mechanics of these pools will be dictated by the developing community.

ROLLOVER POOLS

Linked to each prediction pool, each prediction game has its respective rollover pool. The remains of any accrued yield that has remained undistributed will be available to flow back into yield generating opportunities. The game developer or operator will be able to govern the dynamics of these pools.

4. TOKENOMICS



To ensure the continuous growth of the ecosystem, our native utility token NEZ is equipped with a multitude of features. The core utility of the token is staking, access to tiers, governance rights, pool origination, and the buyback and burn program. Token holders can benefit from such utility by staking the tokens into the Nezha ecosystem or by supplying them for liquidity mining at DEX. Nezha is focused on building infrastructure around yield aggregation and next-generation prediction markets, and Nezha will continue to add and refine token utility accordingly.

PREMIUM TIERS

Firstly, staking NEZ into its native ecosystem enables access to premium tiers to its holders. Such tiers correspond to a premium user experience, only achievable through staking NEZ tokens. Depending on the tier level, premium users are rewarded with extra market entries proportional to their stake in the protocol. Furthermore, staking tokens will give access to premium game pools and early releases. If a user stays a premium member for a certain time frame, this commitment to the Nezha community will be rewarded by receiving exclusively minted Nezha NFTs.

GOVERNANCE

Through staking NEZ, holders of the token gain certain governance rights in the Nezha ecosystem. Token holders will be granted rights that allow participation in governance and administrative decisions, as well as voting on the operational development of the ecosystem. Any token holder who has staked their NEZ within the Nezha platform can contribute a suggested improvement to the ecosystem. All suggested improvements will be reviewed by the board of the DAO and suggested solutions will be proposed to all members. Solutions will be implemented if they achieve a three-quarter majority of votes by all DAO members.

Independent of DAO membership, members will be able to vote on newly submitted games or game proposals by developers. This allows the developer to test any games prior to significant expenditures in marketing and developing them. Nezha strongly encourages all developers to offer special access rights and other benefits to members who have voted on their proposal.



During the second stage of the Nezha ecosystem, staking tokens into the Nezha protocols will enable independent developers to design new prediction market games. Independent developers building on the Nezha protocol will be required to stake NEZ to submit projects, which will be audited, and then voted on by other protocol participants. Besides contributing to the well-being of the protocol through long-term participation, such staking will ensure the growth of our ecosystem, leading to a quickly growing source of entertainment fueled by the inputs of our beloved community.

POOL ORIGINATION

In order to launch the pools required to operate a game, participants will be required to stake a certain amount of NEZ tokens. The exact amount of tokens will be defined at a later stage and will be voted upon by all members of the DAO. Pool origination requests will be voted on by all members of the DAO to ensure that the games launched reflect the best interests of the community.

LIQUIDITY MINING

Nezha will proactively list the NEZ token on several external exchanges which require liquidity to be locked to operate the exchange pool. Liquidity providers will be awarded a percentage of the fees generated in these pools. The distribution of those is not controlled by Nezha but by the operator of the exchange. Nezha will separately reward Liquidity Providers with NEZ as well as stable coin rewards. The mechanics of this are outlined in the section on Liquidity Provider Pools in this paper.

BUYBACK AND BURN POOL

To ensure price stability and value creation for NEZ token holders, a buy-back and burn protocol aims to protect the native token NEZ from price depreciation. Specifically, a small portion of each week's generated yield funds our buy-back and burn pool, counteracting bearish market periods. The Board of the Nezha DAO will propose a buyback and burn initiation on which all members can vote. If the vote is successfully approved as defined by a two-thirds majority, Nezha will manually place buy orders and burn corresponding tokens. This promotes less volatility in token price even during bearish markets, and long-term appreciation of the token's value through reducing the amount of circulating tokens following the rules of supply and demand economics.



TOKEN DISTRIBUTION

Our native NEZ token is at the heart of the Nezha ecosystem and fuels our ability to grow and develop new games. Less than seventeen per cent of all available tokens are controlled by the community of stakers that finance the initial development of the platform. About forty-seven percent of the tokens are in control of the operating team and will be used to fund the development of the ecosystem, provide liquidity on exchanges, and incentivise the team working for Nezha. About thirty-six percent of the total tokens are in the control of the community. To safeguard the stability and health of our ecosystem, we have implemented an eighteen-month vesting period for all stakers as well as a four year vesting period for members of the operating team. Our token distribution has been designed with the integrity and stability of our ecosystem in mind.

EXHIBIT A.)
TOKEN DISTRIBUTION

TOKEN ALLOCATION

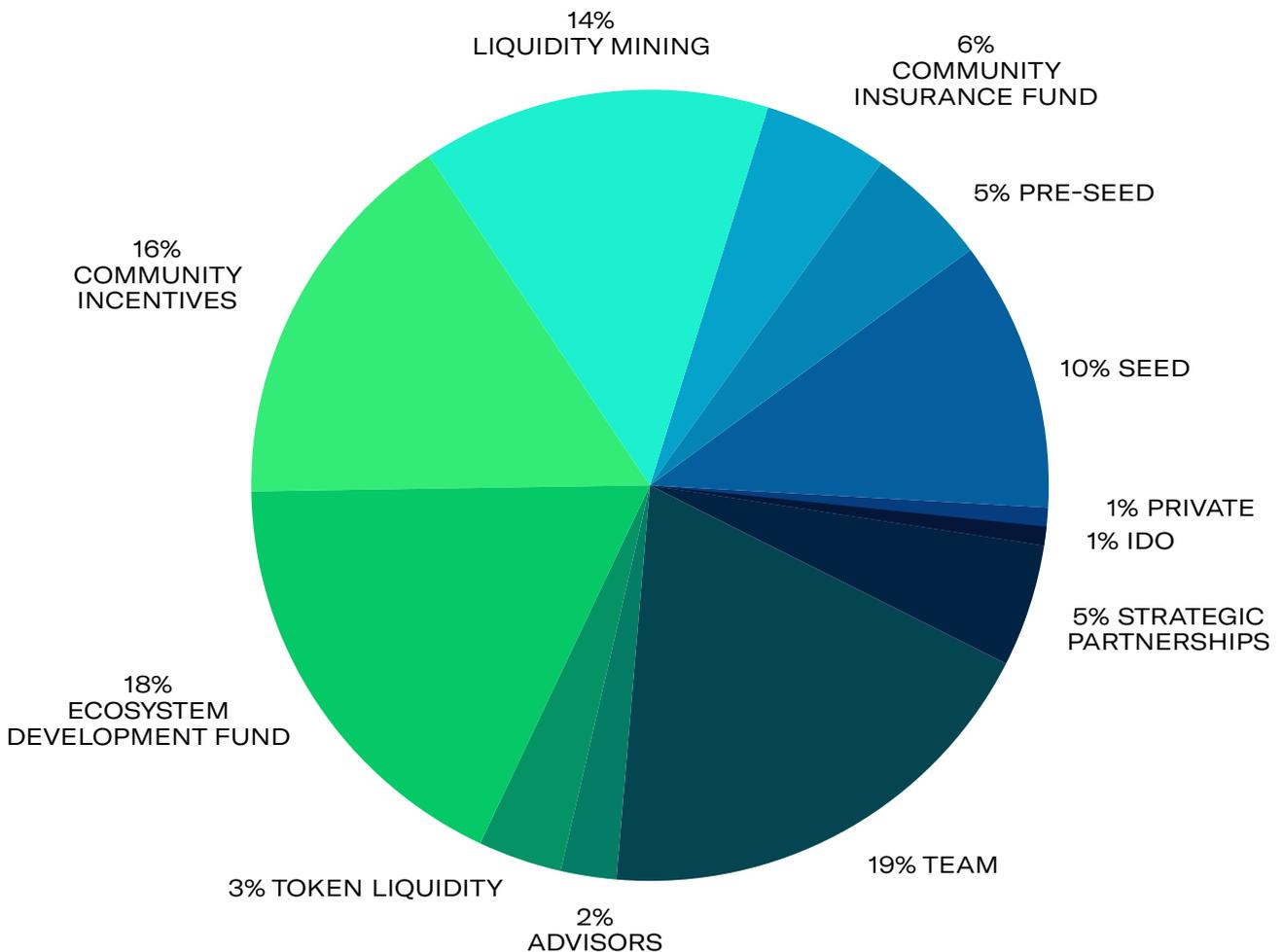
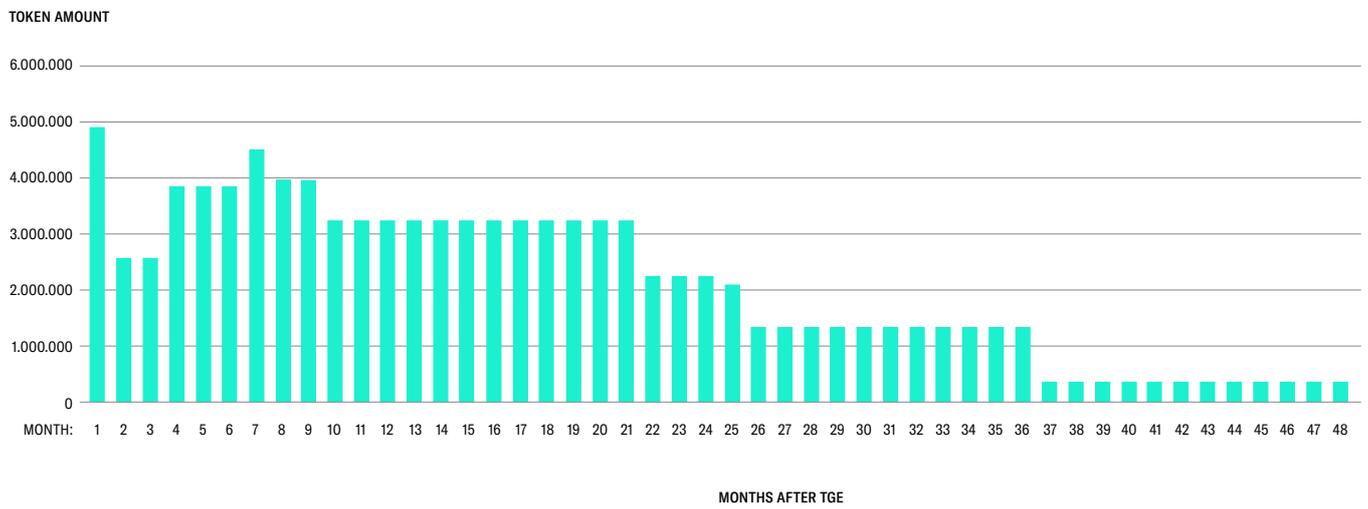




EXHIBIT B.)
TOKEN RELEASE SCHEDULE

NEZ TOKEN RELEASE
SCHEDULE



5. LAUNCH PLANS



After careful consideration, we have decided to develop our protocol for multichain deployment. We will first launch our application on Solana and then deploy to more ecosystems at the earliest date possible. Furthermore, we continuously evaluate novel developments and opportunities for further deployment, focusing on other third generation blockchains. While some competition persists between Layer 1 chains, we recognise the unique benefits of each. We like to remind that each of these Layer 1 chains has invaluable use-cases, and that their sophisticated developments bring our world one step closer towards decentralisation, inclusiveness, and security. We see a close fit with Nezha's values, by aiming to change the world for the better through the power of technology and decentralisation.

Legacy infrastructure has made prediction markets zero-sum driven environments. Blockchain technology allows Nezha to fundamentally reinvent prediction markets, making them a positive-sum game, thereby generating value for all. Furthermore, the innovation in the DeFi sector, and liquidity in third generation blockchains enables novel staking strategies through yield aggregation, which Nezha will bring together through gamification and prediction market activities.

Firstly, we are launching our application on Solana. The growth and development has been unmatched in recent periods due to the fast scalability enabled through its novel proof of history consensus protocol. Through streaming transactions, Solana manages to keep transaction costs low while maintaining high security, benefiting its Layer-2 dApps tremendously. Here, we look forward to launching our first pool, enabling us to provide our offering to the community with accessible transaction costs in due time. The DeFi and GameFi realm has experienced tremendous growth, with an abundance of liquidity and a engaged community awaiting the Nezha application.