



HORUS PROTOCOL





Table of contents

1. Introduction.....	3
1.1 The state of gambling.....	3
1.2 The market.....	4
2. The fix.....	6
2.1 Transparency.....	6
2.2 Even odds.....	7
2.3 No need for cash.....	7
2.4 Connecting people and rewarding skill.....	7
3. Our protocol.....	8
3.1 Bets.....	9
3.2 Staking.....	11
3.3 Bets management.....	12
4. The roadmap.....	13



1. Introduction



We are bringing full transparency to the current betting system; the odds are not stacked against you anymore.

1.1 The state of gambling

Crypto all-ins, online betting and degen stock market plays are more and more common nowadays as these communities gather on the internet, forming slangs and seeing more and more degen plays pay out or totally wipe one's portfolio.

We believe that these systems are inherently flawed and are deceptive. To obtain these gains you'll see on various platforms and online communities, you'll either need to get extremely lucky or to have an edge over the market, and that takes skill and practice.

We want to bring you a way to master your risks and enter the plays that give odds you are ready to play.



1.2 The market

The traditional world of gambling and betting is divided in many categories:

- The traditional casino way: the game is rigged in the favor of the casino, meaning you have less chance to win. Take roulette's zero (zeroes even in some cases). The basic probability of winning while betting on red is $\frac{1}{2}$ but with the zero it shifts to:

$$p = \frac{1}{2} - \frac{1}{37} = 0,47$$

- The most popular way nowadays: sports betting. Here, the trick lies in the odds you are offered by your bookmaker or your favorite sports betting application. The odds are calculated to have you in a situation where you are getting paid far less than the bet is worth. Furthermore, the way the odds are calculated is, in the case of your bookie, sketchy and at best obscure.
- The most degen bets IRL are through bookmakers and once again the odds are the problem as the way they are computed is obscure. An example is betting on the queen's hat color at her next appearance.
- You can also bet with your friends on various subjects (who will have a better grade, who can beat the other one at smash bros, etc....). This method is the most fun one to us, but it has its drawbacks, a party can refuse to pay, and you'll have to get cash most of the time, which is not practical.
- Finally, probably your way if you are reading this: the degen one. With online brokers easily available, anyone can just put all his savings in options, leveraged trading or shitcoins. Let's tackle these examples one by one. Options trading, everything is priced in, and you'll need to have serious experience, do a ton of research and probably get a bit lucky to assess the probability that you'll win anything from investing in these assets. Leveraged trading, especially in crypto, is not suited for beginners and requires a ton of research, experience, trial and error. Finally, shitcoins: you'll need to put in a ton of research, invest in projects that will die or straight up rug. The probability of you gaining anything is hard to assess and you'll probably be more likely to lose money if you are a regular ape.



Drawbacks of the traditional betting system



Betting System

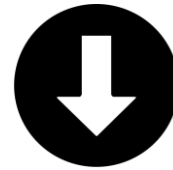
Casino

Sports Betting

Degen Betting on random events

Bets amongst friends

Degen investments



Downside

Odds straight up against you

Obscure odds computation method
Calculated to make you lose

Odds even more obscure
Need cash when going through a bookmaker
Can be used as a front to launder money

No real payment obligation
Need cash

Lot of time required to be able to win
Odds to win difficult to assess



2. How does Horus Protocol fixes this?



For us, transparency is key in gambling. The blockchain is a great opportunity to make it the new standard.

2.1 Full transparency

Horus allows you to have total control over your odds of winning a bet: everything is on the blockchain, the contracts are verified and can be audited by anyone.

At first, we thought of using pseudo random number generation in solidity, but miners can manipulate the variables used to create such numbers (block timestamp, block difficulty etc....). We can not allow anyone to manipulate the outcome of a bet, therefore we had to produce another solution.

The solution to this is to get a random number from a source outside of the blockchain through an API (oracle operators). This solution also comes with a problem: the random source is centralized and can manipulate the numbers it sends us. Furthermore, if the site is down, the contracts are useless.

The fix to this issue lies in Chainlink VRF (verifiable random function). It is a public-key pseudorandom function (the best an algorithm can do), that allows us to provide the proof that the function was executed, and that the computation went as planned. Chainlink's VRF allows us to access pseudo randomness without any problem of security, a proof of how that number was generated is published and verified on chain to ensure that the results can not be tampered with, thus guaranteeing the random aspect of the game.



2.2 Even odds for everyone

Our motto is to offer the possibility to anyone to take a calculated risk with his money, purely speculating that one can win and master the odds.

You are risk averse and are trying to triple your money in one go? Horus can provide you a 1:3 chance of tripling your money, for a small fee.

Everything is transparent, you can check our contracts, see that they do call the VRF function and check that the probability we claim you have to win is correct. No knowledge is needed, this is just about the risk you are willing to take and the thrill you will get while doing so.

2.3 No need for cash or shady transactions

Everything happens on the blockchain, no need to make non-refundable deposits to an application or a shady online casino nor use your credit card to do so.

The transaction is made through your online wallet via the press of a button on our site, it does not really get quicker than that.

By acting as a fair bookmaker and bringing the easiest-to-use service, we want to bring betting on your luck the easiest way to earn money.

2.4 Connecting people and rewarding skill

Of course, our ambition is to go beyond the pure luck aspect of the first games and betting mechanisms that we will release. We want you to be able to earn money through the games you are good at.

Having a friendly argument on Discord with your friend and you want to settle who is the superior human and are both so confident that you'll win that you are ready to put some money on it? Here is Horus, providing you a reaction time test that'll settle the argument through a money match.

You think you are better than average at something? Well test yourself through a matchmaking system that will allow you to try and beat most of the players you face to earn from your skills as a player!



3. Our platform



We want the user experience to be as fluid as possible to allow our clients to focus solely on their game plan.

Our protocol is built around three key features:

- 1. Betting**
 - 2. Staking**
 - 3. Bets management**
-

Our platform will be at first available on Polygon as it is a fast and reliable blockchain, with low fees.

The VRF implementation on this chain is also cheaper than on Ethereum, Binance smart chain and other competitors. Our goal is to expand to different chains (Avalanche, Fantom, Ethereum, Binance Smart Chain...).

But for now, as security and transparency are the most important features for us, we prefer to keep it to Polygon to guarantee low fees to our users.



3.1 Betting

The bets regroup all events in which a player will rely on mastered odds (simple bet or lotteries) or on his own skill (bet amongst friends, matchmaking, tournaments...). This generates yield for the protocol through fees (3%).

This feature is quite straightforward: every time a player decides to bet on our protocol, he must pay a 3% fee. This rate applies to the simple bets like double or nothing as well as the lottery.

At launch: the available bets will be the instant ones where the player decides on his odds and bets a certain amount. The protocol makes a request to Chainlink's VRF to get a secured random number that no one can manipulate. This feature ensures that neither the team nor a third party can influence a bet's result. The drawback of this method is that Chainlink's VRF can be slow at times and take up to 40 seconds in its V1. Furthermore, every request costs a small fee paid in \$LINK, that the protocol will have to pay for every bet, these costs will be paid for by the team. This is the price to pay to guarantee that our random numbers can not be tampered with.

We are waiting for the V2 launch of Chainlink's VRF on Polygon to launch the protocol as the average waiting time would go from 40 seconds to 20 seconds, effectively enhancing the user experience on Horus Protocol.

For every bet, a specific contract is used, and we use modulo to convert the large random number into a probability. We are aware that the modulo function is inherently flawed but working with very large numbers negates this issue.

For every winning or losing bet, each one of these contracts centralizes the fees in a contract and interacts with the protocol's treasury to pay the user or collect the winnings.

Now, one question must come to your mind: how are you going to pay the users? Usually, similar projects launch an NFT collection, and their pool is made of funds coming from the mint. We are different: the liquidity will be added by the team, and we are putting our own money at risk, not yours.

Using a binomial distribution, we can compute the probability of the pool getting drained over a fixed number of bets with a fixed bet price.



Let's take the worst-case scenario and assume that everyone bets the max amount allowed by the protocol: 50 \$MATIC.

We have seen similar projects computing the following formula to compute this probability (in the case of a coin toss):

$$p = 2^n$$

With:

- p the probability of that event happening
- n the number of consecutive events

This formula represents the case where their pool gets drained in one go, meaning that every bet would be losing for the protocol without any winning one. This is obviously flawed and does not consider the cases where winning bets occur in between losing ones.

To compute the real risk of getting your pool drained, you must fix the number of bets you want to study your resilience on. We chose 4500 bets as it is the worst-case scenario (see the Annexes to get a better explanation of our reasoning).

Skipping over some details, we use the binomial distribution formula to compute the odds of our pool containing less money than at the start after 4500 bets: 2,21%.

This seems high but we basically consider that the money we put in our pool is not ours anymore, so it does not matter. What really matters is: will we be able to pay our players in an event where we get unlucky? The probability of the pool to get drained in 4500 bets is: 0.00054%.

This represents a chance on 188,000 of happening, this is extremely low, and we believe that this is an acceptable probability.

Our top priority at launch will be securing as much as possible the protocol by regularly increasing the size of the liquidity pool. This will allow us to increase the max amount per bet and ensure further that the pool will not get drained.

For the lottery feature, no pool is required as every lottery ticket will have a fixed price and the winner will get paid the sum of these tickets, minus a small fee taken by the protocol for fees and Chainlink's VRF use.



3.2 Staking

In order to pay the users, the protocol will have its own liquidity. This liquidity will be kickstarted by the team and will be increased regularly to allow the protocol to pay its users in more high-stake bets.

Part of this yield will be redistributed to a selected group of liquidity providers.

Our system is the following: to guarantee a high yield to our investors, we must limit the number of people that will be allowed to provide liquidity.

At launch of the staking feature, the tokenomics will be the following:

- Number of stakers: 50
- Max allocation: \$500
- Total allocation: \$25,000
- Rewarded tax: 0.5%

Let's say you decide to put \$500 and the total allocated is \$25,000, you own 2% of the liquidity open to investors. Let's assume 1,000 bets of 30 \$MATIC are done in a day (compared to the Degen Coinflip standard it is very low as approximately 25,000 flips are made on a day-to-day basis). 30,000 \$MATIC are bet, you get a 0.5% tax on this and get 2% of this. This means you earn 30 \$MATIC (as of today \$50), which means you earn a 10% yield DAILY, meaning the APY of this investment is 3650% with only a thousand bets daily (not counting the other features).

How will the stakers funds be used? The funds stakers invest in Horus Protocol will be used to secure the liquidity pool of the project, guaranteeing its resilience and allowing us to increase the max bet amount per bet.

With this staking, no risk is assumed by a \$MATIC holder because they stake \$MATIC and get rewarded in \$MATIC. A small fee is harvested when one decides to unstake, this is all the downside an investor can fear: 0,5% ONCE (1/20 your daily yield if computing the case, we just detailed).

We plan on increasing slowly the max number of stakers allowed and open two programs: one closed and one open. The closed one will have a staking limit and a low investor count to bring a high APY. The open staking program will launch once we feel the protocol is stable, its goal is to open to everyone part of the rewards of the protocol. Obviously the APY will be lower than the closed program, but the added liquidity will be used to develop new games and open to new blockchains.



3.3 Bets management

Now addressing the most critical point about our project.

We have had the opportunity to see what excessive gambling does to people and this is not something we wish on our investors and players.

Therefore, we decided to create a ban list. If you feel that you have a problem with keeping control over your betting, we advise you to signal yourself to us and we'll take measures to ensure that you can not bet anymore.



4. The Roadmap



The protocol at launch is destined to be outdated quickly as our main focus is building upon this foundation, here is our plan.

Our plan is to launch the protocol with a few features and extend upon them. The first features will be a double or nothing and triple or nothing bet and the lottery.

First plan of action is using some of the fees for marketing, more users means more fees and more rewards for our stakers.

Once the protocol is relatively stable on Polygon, we want to go to other blockchains, mainly Binance Smart Chain and Avalanche. For now, we feel the VRF V2 fees on the BSC are still a bit high and we would have to only offer bets of over \$100 for us to pay for the transaction, which requires quite a big liquidity pool. For Avalanche, no VRF is implemented yet and we are waiting for it to expand to it. Cross-chain means more users and more rewards, we will implement a separated closed staking program on every chain we expand to.

In parallel, we'll keep on adding simple games (bets based on odds mainly and augmenting the max bet on every game depending on the treasury). The main goal here is to listen to our community and implement the games that the community wants to have.



These three axes of development will be tackled instantly after launch and are crucial for the next step. As we said, our goal is to become a gaming platform. Our goal is to have users create rooms and invite friends to play multiplayer games for money. We want to keep a random aspect in some of them (rock/paper/scissors for instance) and have others be dependent on skill alone (reaction time, typing speed...).

The first feature to be implemented is the creation of an account and the creation of a rock/paper/scissors game, with an invite link and a fixed bet between the two players. Expanding on this, we'll create a matchmaking system to pair two players randomly for a game, using a fixed bet size.

Once this feature is tested and implemented, we'll add the reaction time game, adding an Elo system to the matchmaking system so that one can grind through the ladder and earn money from his reaction skills. Every new game will be playable through random matchmaking and through private rooms.

The next step after that will be to consolidate the existing system, fixing issues as they come, and start adding more games, typing speed, chess, requests from the community...

Once this system is stable, we want to federate the community through regular events: tournaments.

For every player willing to take part in the tournament, there will be a fixed entry fee that will go into a pool to reward the top players at the end of the event. Every tournament will be broadcasted and commented on to add pressure and create a hype event. Rewards will be much higher than the ones from a regular bet and skilled players could see a huge upside.

Once this system is implemented and stable, we'll launch a DAO with a governance token that can be obtained through playing on the platform. It could be exchanged for free bets or used for governance questions (fees taken by the platform, number of closed stakers, games implemented, chains expansion...).

Through all this process, a portion of the collected fees will go to marketing (influencers, giveaways, articles, collaborations etc....)