* Video Transcript

Fair contest & Transparent Probability Model

Have you ever wondered if the probability of getting virtual treasures that game companies disclose is true or not? As players, we cannot prove the truth behind the probability provided by game companies. So, that's why we're here! We'll write these probability models on the blockchain so that everyone can verify if the probability is really what the company claims! Additionally, if you win a big prize today, will you tell everyone? We have taken this into consideration, and we'll use Zero Knowledge Tech to protect your identity and privacy.

Let's introduce our model! First, our users use two random variables, KEY and SECRET, to calculate a variable called Commitment. Then, they pass this parameter into the contract.

Then, we'll use two random functions to determine whether the lottery is a winner. Next, we'll store the result in the corresponding contract to obtain a Merkle tree's root value. This ensures that third parties don't know what the winning information is. So, the second steps is end.

Next, if a user wants to confirm what prize they won, they need to interact with the chain, using the Merkle tree's root parameter to scan the Merkle tree in the contract to see if it contains the value. If the value exists, it confirms what the prize is.

If you don't want to confirm what prize you've won, to save gas fee, you can just withdraw it directly! We designed this method because some people may win big prizes but don't want others to know. They can isolate their wallets to prevent others from tracking there address to find who they are.

Our lottery model has a fixed probability for each draw and it does not change even if a prize is won.

For example, if USERA spends 30 USDT to participate into a lottery game and the chance of winning 1BTC is 1%, and then USERA actually wins, the probability of winning 1BTC for USERB in the next draw, the chance to get 1BTC will still be 1% and does not change.

After considerable effort, we have deployed the program on Gnosis, ThunderCore, and ETH Chain.

The advantage of this idea is that users can see transparent probabilities, which may increase their willingness to participate in the game, leading to a significant increase in participation rate.

However, the disadvantage is that the prize quantity needs to be limited or the probability needs to be adjusted, otherwise, the project may suffer from high losses.

Finally, we can provide this model to gaming companies as a reference for future promotions or for large-scale event lotteries.

* Project Description

1. Addressing players' concerns regarding winning probabilities.
2. Ensuring high-level confidentiality of winning information.

* Team Description

Andrew Chang: Studying for a Master's Degree in the NYCU CSIE Department, responsible for front-end development, presentation reports, and conceptualizing video editing.

Peter Chang: Studying for a Master's Degree in the NYCU CSIE Department, responsible for smart contract development.

Henry Lai: Studying for a Master's Degree in the NYCU CSIE Department, responsible for smart contract development.

Matin Lai: Studying for a Bachelor's Degree in the NTUST CSIE Department, responsible for developing intelligent pages.

* Category/Tags:

Zero Knowledge Proof