Distributed Trust & Blockchain

smart contract for a quiz

October 2018

Why smart contract for a quiz ?

A Decentralized Quiz Platform where participants and quizmaster can function without having to trust each other, but trust the contract which is visible to all.

Rules :

1. N number of people participate in a single game of 4 questions.
2. Each person pays a participation fee (*pFee*) before entering the game.
3. Let *tFee* denote the aggregated some of all the participants' fee in the game.
4. For each correct answer a participant gets 3/16* *tFee* reward. That is, the contract earns a quarter of tFee in each game.

Goal :

- Figure out all the security measures required to implement such a system
- Game should be fair & justifiable
- Test cases should be robust

Method Followed :

1. Quiz master will specify number of players and registration fee. Then the contract is launched.
2. Users can register using registerplayers method. User needs to provide his answers
3. Once all users are registered, Quiz master will give the correct answers.
4. Then the pickWinner is called. Here's how it works
   For each player, it calculates the score by comparing it with answers. If there are more than one players with correct answer, the reward is given to first player who has answered that question, based on timestamp. Reward is given using formula given above.

5. Once all the rewards are calculated and stored, players can claim their reward earned. Quiz master will take away whatever balance is remaining after all reward payments. Essentially, this would be (¼)*tFee*

Test Cases :

- No registrations should be allowed after specified number of players are registered.
- Participant should pay exact amount of *pFee* demanded by Quiz Master. Not more. Not Less.
- Address of Quiz Master and Players must be a valid one.

To Do :

- FCFS is followed while rewarding, can do something better and more fair here.
- A player's answers shouldn't be visible to anyone including Quiz Master. Some sort of encryption would do. Using address, timestamp and answer as seeds.
- In addition to limitation on number of players, a timestamp can be added after which registrations are closed. Another timestamp can be used only after which users can register.

References :

- Related to Ether and Payment ; A basic banking template