COMP6451 T1 2022

Assignment 2

Haozhe Chen

z5142012

**Part 1: Contract structure overview**

This assignment can be divided into two parts of contract:

1. Share contract use ERC20 standard interface
2. ICO (initial coin offering) contract which is used to collected ether and grant shares (tokens)

图示

描述已自动生成

**[Round 0] Initial**

In this round, beneficiary (aka NeverPay company), will deploy the ICO contract (NeverPayICO.sol) into the blockchain. In the ICO contract’s constructor, the share contract (ERC20NeverPayToken.sol) will be initiated.

Before this round end, the ICO contract should keep 10000 tokens.

**[Round 1] Bid**

In this round, investors are able to call bid function to make a blinded bid. The parameter should be a hash value = keccak256(share, value, nonce).

**[Round 2] Reveal**

In this round, investor will call reveal function to open their bid in round1 and pay to the contract. The parameters are shares, value and nonce.

If hash value of these three parameters is equal to bid record in round1 and amount paid is larger than price \* shares, this reveal is successful. Otherwise, this reveal is failed.

**[After Round 2] Issue**

This round is used to let every investor to get their shares and refunds. Beneficiary can also call this function to get ETH collected during the last round (only successful bid).

The issue function will firstly sort every bid (reveal successfully in round2), then the successful bid’s owner will get the shares, failed bid’s owner will get the refunds.