CehhCoin

Hiro Inu

February 20, 2018

1 Introduction

Tokens are premined or minted. People who want a proof of work coin need to launch their own blockchain.

2 Concept

CehhCoin is essentially an ERC20 token with added pseudo proof-of-work capabilities. The idea is simple: all addresses have a certain amount of CehhCoin.

3 Concept Description

All addresses are credited an amount equal to the last 7 bits of the address. At a price P, users who want to mine CehhCoin need to test private keys of Ethereum addresses until they find an address with a balance Q such that PQ is higher than the transaction fee for funding the address and evacuating the tokens to a personal address.

Humans want things to have a purpose, even if sometimes the purpose is just because. The purposes of CehhCoin, if you want some, are the two following:

1. Begin the end of trash blockchains.
2. Have a pseudo-standard way of seeing gas prices in average human terms i.e. dollars.

If this PoW standard is developed further, then point 1 would be accomplished. Adopting this standard would make utility blockchains able to migrate into Ethereum and benefit from its continued development.

The second point could be more interesting, because in general the idea of gas prices stays somewhat abstract until users try to send a transaction. The way CehhCoin gets its price comes from the inherent cost of token mining. There are a few factors that come into play to determine this gas cost pricing. First we have the spending required to claim tokens. Claiming different amounts does not affect the price of the function call. Let this price be C. There are also costs associated to moving the ETH required to execute the transaction. Moving the ETH has a fixed gas cost of 21000 gas limit. This price is T. On the other hand, the markets have their own prices. CehhCoin will have a certain price P. This price will be determined by arbitrage opportunities. CehhCoin is designed as a hedge currency.

In the first place, the cost of mining $C + 2T$. The user needs to transfer ETH to the account with CEHH, then claim, and finally evacuate the tokens. The decision to either mine or not mine comes from the price at which the tokens found may be sold. Given a price P, the miner can finally obtain a profit

$$R = PQ - C - 2T.$$

We then have price stability when $R = 0$, so the price of the token is

$$P = \frac{C - 2T}{Q}.$$

It can happen is that $C - 2T$ go up due to gas prices. At a fixed ETH price, gas prices will impact the mining cost in a linear way. That is, if gas prices increase in α, the mining operation goes up in α as well. When gas prices go down, α is less than 1. In that case the new equilibrium is reached at

$$\Delta P = \frac{(1 - \alpha)(C + 2T)}{Q}.$$

There are two scenarios. Either $\alpha > 1$ or $\alpha < 1$. When $\alpha < 1$, mining becomes cheaper and $R > 0$. The supply then goes up and eventually the price stabilizes via arbitrage opportunity.

The more complex case arises when $\alpha > 1$. This means that mining more CehhCoin would happen at a loss. This keeps the price fixed at P as the supply doesn't change (by assuming people don't sell at a loss.) The case where $\alpha > 1$ is related to network clogging and higher transaction volume. Transaction volume is related to volatility and network events. As a hedge currency soft-pegged to the movements of gas prices, the movement direction of CehhCoin would be decided by the degree of fear of the market and the effect of irrational human judgment, added to price manipulation.

4 Pseudo Proof-of-Work

The central idea around pseudo proof-of-work (PPoW) is that even in a public blockchain, there is at least 1 secret component: private keys. Previous attempts to create PoW tokens included naive PoW and public and private key pairs. Both of this solutions have problems of their own. Specifically the naive implementation of PoW tokens fails with gas price rushing. The problem with using private and public keys is redundancy and the required know-how.

What PPoW proposes is an airdrop hybrid which becomes a PoW mining system. As stated in the CehhCoin white paper, the price of CehhCoin should be tied proportionally to the price of calling its mining functions. The amount Q is the average amount that miners find. However, a supply and demand setup appears when we find two different Qs. We have the average miner or airdrop participant with a Q_0 and we have miners who have a $Q_1 > Q_0$. The existence of this difference creates a price gap in which people who are able to mine average of Q_1 CehhCoins per call take the role of suppliers over the those with access to a Q_0 average.

The way a miner achieves a higher Q is by being able to test more addresses. The operation needs to be able to offset the cost of mining such that $R = PQ - (C + 2T) - M$ gives $R > 0$. This mining process of PPoW is done by generating random private keys and mapping them to their respective ETH addresses. For the specific case of CehhCoin, the reward of mining a certain address is equal to the value of the las seven bits. With this airdrop-style PPoW there is no need to worry about gas price rushing or about implementing public key checks.

Further research is required to determine if the current 7-bit reward is effective or if further incentives are required to move miners into the token mining system. Another point to place under scrutiny is the actual utility of PPoW aside from reducing clutter in the blockchain space. A clear advantage of the PPoW system is that multiple PPoW are mined simultaneously. Instead of wasting time switching between blockchains, users can mine different PPoW tokens at the same time, as long as the contract interfaces are relatively similar.

In terms of the advantages PPoW offers for the token space are

1. **Asynchronous mining**: rewards are already set in place. For that reason, miners aren't rushing to find the rewards and the network doesn't die or suffer from hashrate fluctuations.

2. **Bundle mining**: as more tokens adopt the ERC 891 extension, they will be able to be mined simultaneously. That means that instead of each crypto requiring its own blockchain with wasted resources most of the time, all tokens can be mined at the same time: each address that miners check can check all the ERC 891 compliant tokens.