CehhGold

The Mineable Token

by Cehhiro

1 Introduction

Ethereum is a smart contract platform. Its native token is called ether, which is used as an economic incentive to keeps things running smoothly. (Usually.) Ether, however, is often used as a currency. On top of Ethereum there are non-native tokens, the most common being the ERC20 implementations. ERC20 works well in small scale, where all the supply is premined and subsequently distributed. Over time, ERC20 was abused by groups shielded under the legal framework of foundations. The old ERC20 standard was extended without changing the name to implement crowdsales. Different foundations used different emission methods, but at the core ERC20 crowdsale contracts credited an amount proportional to the ETH sent. Investors saw a pattern around ERC20 initial coin offerings: the price they had to pay during the auction often doubled or tripled when the token was added to exchanges. From a mercenary-investor's point-of-view this was a golden opportunity. Over time users grew more and more skeptical of ICOs. Not only were these foundations underdelivering, but they had also "unfairly" profited from the ether they raised, as well as their own "team allocation" of tokens. This scheme transferred over 1,000 million dollars worth of ether to just 6 foundations, without taking into account the team self-allocation of tokens.
The name of ICOs has been berated down to scams. Something which was built back in 2016 slowly turned into a Ponzi-scheme enabler, forever denting blockchain-users' trust. Even if new projects come along which require funding, trust has been broken. This idea that the foundations reaped millions of dollars without being legally bound to deliver any product, on top of creating a Ponzi scheme, is still very fresh in the minds on blockchain enthusiasts. This leaves us with the question that ICOs originally answered: how can a developer distribute a DApp token?

2 Mining Tokens

When modern promises fail us, taking a step back is often a good way of solving the problem. In this case, we move out of ICO schemes and go back to mining. It was with this idea of taking a step back that ERC891 came up. If a DApp developer requires a token because ether itself isn't

enough, implementing ERC891 would allow for organic growth of supply and user base. A successful project would have expanding supply, while an abandoned project would freeze.
The way ERC891 works is via address mining with ECDSA signatures. Addresses themselves already contain unclaimed balances of ERC891 tokens. The amount that each address may claim depends on the address's hex value itself. The principle that makes this possible is that it is not possible to guess a specific address's private key. Instead, users mine addresses until they find one with an amount that lets them claim it at a profit. The tokens will grow and fall in value as much as people actually perceive their worth.

3 CehhGold

The first contract to fully implement this idea is CehhGold. The token amount given to each address follows a simple rule: finding an address ending with 72 consecutive bits holds 50 CehhGold a.k.a. CEHH+. Each bit under 72 halves the reward held by address. This means that a 71-difficulty address holds 25 CEHH+, and a 70-difficulty address 12.5 CEHH+. Since claiming the reward from a mined address has a fixed offset cost, mining one 32-difficulty address is more profitable than two 31-difficulty addresses. This multi-level difficulty system also serves as a workaround for mining pools, allowing even mobile users to obtain rewards that fit their mining capacity. Furthermore, mining addresses doesn't require the immediate submission of the signature or claiming of the balance; this can be delayed indefinitely until the user can access ether or sells the signature off-chain.