The Revenue Token

The Concept

ICO | We Mine Currencies | Distribute profits

The Challenge #1

Keeping track of tokens once they leave the ICO wallet, and are stored in hot/cold wallets.

The Solution #1

An ethereum smart contract that '**knows**' about all current token holders by storing a **list of all token holding addresses**.
Every month(or fortnight, your choice), you update the smart contract of your earnings for the period.
The contract then tracks every account holder and awards dividend(in terms of ETH) in proportion to the account balance.

Gas Limit Estimates : 2,000,000 (for moderate number of users, increases linearly with number of users)
Gas Price Estimates : the SafeLow on https://ethgasstation.info/ should work fine. (1 Gwei at the time of writing, may fluctuate over time)

Pseudocode #1

```
function disburse(int amount)
{
    deduct(msg.sender, amount);
    for i in accounts:
    {
        balance[i] += (amount * balance[i]) / totalSupply
    }
}
```

The Challenge #2

The contract has to do **work proportional to the number of token holders**, which means that as the number of token holders increase, your **gas costs rise** and you rapidly hit the block gas limit on the blockchain.

The Solution #2

Instead of updating every user's account at once at the time of disbursement, we can keep **track of the total dividends**, and add a user's pending dividends when there's a transaction against their account.

Gas Limit Estimates : 21,000(by you) + 21,000(per account by the account holder)
Gas Price Estimates : the SafeLow on https://ethgasstation.info/ should work fine. (1 Gwei at the time of writing, may fluctuate over time)

Pseudocode #2

```
//code redacted for reader's sanity
```

Security Concerns

The following are a few initial security concerns associated with the contract:

1. Rounding errors
    - We assume that the dividend can be evenly divided across all accounts. This may not be always true, resulting in a few wei lost to rounding errors.
2. Orphan accounts
    - We may want to tackle the problem of Inactive accounts receiving dividends indefinitely.
3. Double disbursement against the same token
    - We have to ensure that a fraudulent user is unable to disburse against the same token twice in a single payout