# NuCypher KMS: Mining

Michael Egorov[*]
*NuCypher*

(Dated: January 11, 2018)

This paper describes mining mechanisms and economics in NuCypher KMS. It includes inflation rates, mechanisms to incentivise long-term stakers and estimates of number of coins generated by nodes running in typical modes. Also, optimal strategies for stakers who may be affected by market volatility are proposed.

## I. MOTIVATION

In future, NuCypher KMS will probably be fully paid by network fees. But initially, when the adoption isn't yet high, miners who run the nodes necessary for network operation and keep re-encryption keys, will need to be subsidised. This will be done through inflation schedule, where all the inflation is given back to miners.

The individual inflation rate will be dependent on the minimal time $\tau$ the node commits to mine for. It will incentivize longer miners. The coins staked at this time will be fully available in no less than the time $\tau$.

Mining rates, however, shouldn't be overly too high: too high inflation schedules may depreciate the price. For example, the price of ZCash experienced an inflection point (started going up) only when it become lower than 350% APR. However, for steam.it, the inflation rate of about 100% per year appeared to be too high. Hence, to be on the safe side, our inflation should be lower than 100% per year, and also we should provide convenient ways for miners to restake what they mined. If the restaking happens automatically, so that what is mined isn't even taken out of the smart contract, it could have tax advantages in some jurisdictions also.

## II. DISTRIBUTING REWARDS BETWEEN STAKERS

Let the daily relative inflation rate be $\varepsilon$. If all the miners had the same rewards rate, the profit of individual miner is:

$$dc_i/dt = r_i = \frac{s_i}{\sum_i s_i} \varepsilon C, \tag{1}$$

where $s_i$ is stake of an individual (actively staking) miner, and $C$ is the total number of coins currently in existence. Rate $r_i$ is the increase of the number of coins the miner has $c_i$ per day.

## III. INCENTIVES TO CREATE LONG-TERM STAKERS

Our network needs nodes which can live up to a year, to handle long-term re-encryption policies (although longer than a year could be not necessarily good in terms of incentivising key rotation). Thus, we have to provide higher rewards for people who stake for a longer time.

The daily reward rate coefficient $\epsilon$ depending ...

## IV. INFLATION MODELS

## V. POSSIBLE STRATEGIES FOR STAKERS

## VI. EDGE CASES: RESTAKING DURING UNLOCKING, CONNECTIVITY PROBLEMS

[*] michael@nucypher.com