NuCypher KMS: Mining

Michael Egorov*
NuCypher
(Dated: January 31, 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.

Distribution of rewards should have the following properties:

- All the inflation is distributed to stakers who run the nodes, proportionally to the stake;
- Amount of work (and, hence, the fees) is proportional to stake also;
- Stakers are incentivized (by a higher reward rate) to run long-term nodes;
- High inflation doesn't depreciate the price in order to keep liquidity good for new stakers;
- Stakers are incentivized to stay online all the time.

In the paper we address all these points, calculate expected earnings of miners who run nodes and devise optimal mining strategies.

II. HISTORICAL EXAMPLES OF INFLATION

Let's review inlation schedules of different cryptocurrency projects: DASH [1], ZCash [**?**] and Steam.it [**?**].

Dash has a hybrid of Proof-of-Work (POW) and Proof-of-Stake (POS). It has 45% of inflation going to POW miners, 45% to staking master nodes and 10% is reserved for budget proposals [2]. After the first year, its emission was 18.42% APR, decreasing by 1/14 every 383 days. With this setting, 60% of DASH coins are locked in masternodes for staking, according to the node statistics.

[1] Evan Duffield and Daniel Diaz, "Dash: A privacy-centric crypto-currency," (2015).
[2] "Official dash documentation: Emission rate," .

* michael@nucypher.com