# Dusk Network Economic Model Paper

Toghrul Maharramov
Dusk Network
toghrul@dusk.network
version 1.0.1

November 10, 2020

**Abstract**

The document outlines the economic model of the Dusk Network protocol utilized to incentivize participants of the network to preserve the security of the protocol.

# Contents

# 1 Introduction

Dusk Network is a privacy-preserving, distributed ledger-based protocol, which leverages the power of novel cryptographic techniques to strike a sweet spot between efficiency, security and scalability. The protocol utilizes a token called *DUSK* to incentivize consensus participants and to reimburse the participants for the computational costs in the form of transaction fees. Dusk Network is secured via a novel Proof-of-Stake-based protocol called *Segregated Byzantine Agreement* (SBA from hereon). SBA defines two consensus participant roles:

1. *Generators*, responsible for forging and propagating the candidate blocks. Generators play the role of *round leaders* from classic distributed systems literature. Generators are extracted via a so-called *Proof-of-Blind Bid* procedure, which preserves the identity and stake of participants. To become a Generator, the network participant is required to lock-up a certain amount of DUSK in the form of a *bid*.

2. *Provisioners*, responsible for finalizing the candidate blocks propagated by the Generators. Provisioners play the role of *replicas* from classic distributed systems literature. Provisioners form committees, within which they vote for the candidate blocks in iterative steps. To become a Provisioner, the network participant is required to lock-up a certain amount of DUSK in the form of a *stake*.

For each successful round $r$, where $r$ is equivalent to a block height representing a single block $B$, a single Generator and 192 Provisioners are rewarded for the finalization of the block. The winning Generator is defined as the proposer of the finalized block for round $r$, and the winning 192 Provisioners are defined as the members of the 3 committees responsible for the finalization of the block for round $r$. Please note that a single Provisioner can be extracted multiple times per committee, as each staked DUSK is treated as a unique participant, regardless of whether the owner is the same or not.

The paper defines the model utilized to incentivize network participants to adhere to protocol rules and secure the network against posterior attacks.

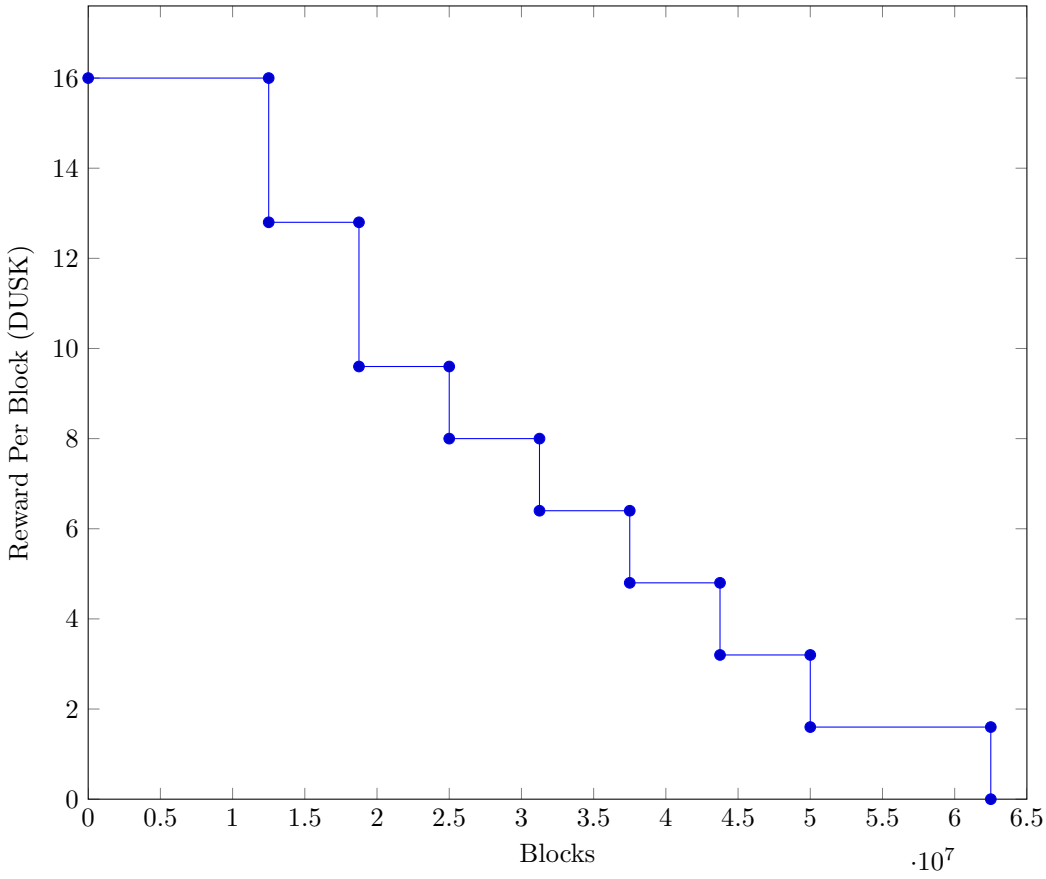
# 2 DUSK Emission Schedule

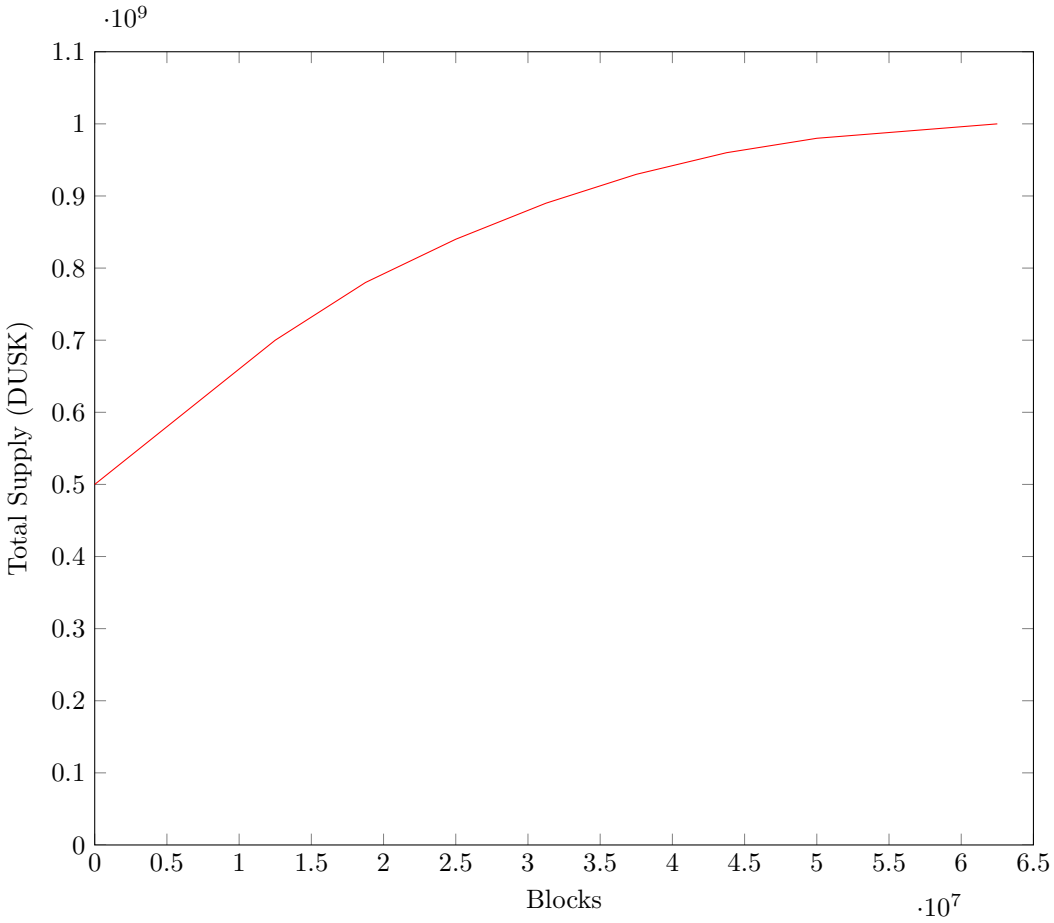
Dusk Network protocol utilizes a token emission schedule to subsidize the costs of securing the network for the consensus participants. While it is natural to anticipate that the accrued transaction fees would eventually become sufficient to cover the costs of securing the protocol, the early days of the protocol would require token emissions to supplement the accrued transaction fees. The token emission schedule is defined in the following table:

| Block Interval | Emission Per Block | Total Emitted Amount | Total Supply |
|---|---|---|---|
| 1-12,500,000 | 16 DUSK | 200,000,000 DUSK | 700,000,000 DUSK |
| 12,500,001-18,750,000 | 12.8 DUSK | 80,000,000 DUSK | 780,000,000 DUSK |
| 18,750,001-25,000,000 | 9.6 DUSK | 60,000,000 DUSK | 840,000,000 DUSK |
| 25,000,001-31,250,000 | 8 DUSK | 50,000,000 DUSK | 890,000,000 DUSK |
| 31,250,001-37,500,000 | 6.4 DUSK | 40,000,000 DUSK | 930,000,000 DUSK |
| 37,500,001-43,750,000 | 4.8 DUSK | 30,000,000 DUSK | 960,000,000 DUSK |
| 43,750,001-50,000,000 | 3.2 DUSK | 20,000,000 DUSK | 980,000,000 DUSK |
| 50,000,001-62,500,000 | 1.6 DUSK | 20,000,000 DUSK | 1,000,000,000 DUSK |

Table 1: DUSK token emission schedule

The table above can be visualized in the following two graphs:






# 3 Definitions

## 3.1 Costs

Each participant of the Dusk Network protocol accrues a certain resource expenditure in terms of hardware costs, electricity bills, internet connection costs, etc. The costs are categorized into two following types:

1. **generator cost**, $c^G$, the costs accrued per round by a user running a Generator node participating in the consensus.
2. **provisioner cost**, $c^P$, the costs accrued per round by a user running a Provisioner node participating in the consensus.

The accrued costs for each of the outlined type should adhere to the following definition: $c^G > c^P$, where $c^G - c^P = \texttt{negl}$.

### 3.2 Node Ratios

The ratio between the cumulative number of Generators and Provisioners participating in the consensus during a single epoch is vital to retain the desired decentralization properties of the protocol, while simultaneously providing optimal performance metrics. The desired ratio $\rho$ is represented by the following function:

$$\rho = \frac{|G|}{|P|} < 1$$

where $||$ denotes the cardinality of a given set, $G$ defines the set of Generators eligible to participate in a given epoch of the consensus and $P$ defines the set of Provisioners eligible to participate in a given epoch of the consensus.

### 3.3 Rewards

For the incentivization model to remain viable, the following two assumptions must hold:

**Assumption 1.** For any Generator $G_i$, which is in possession of a bid $b_i$, larger or equal to $b_{min}$, the reward for participating in the consensus should be higher than the cost of participation per round $c^G$:

$$\frac{b_i}{b_t} \times R^G > c^G$$

where $b_t$ is the cumulative amount of DUSK being bid.

**Assumption 2.** For any Provisioner $P_i$, which is in possession of a stake $s_i$, larger or equal to $s_{min}$, the reward for participating in the consensus should be higher than the cost of participation per round $c^P$:

$$\frac{s_i}{s_t} \times R^P > c^P$$

where $s_t$ is the cumulative amount of DUSK being staked.

## 4 Reward Distribution Per Block

Each block includes a reward, $R^B$, which is distributed amongst the consensus participants responsible for the finalization of the block for round $r$, $R^N$, as well as the *Dusk Network Development Fund*, created with a goal of incentivizing the community contribution to the development and maintenance of the protocol, $R^D$. $R^D$ will be allocated to the Dusk Network Development Fund for the first 12,500,000 blocks, after which $R^D$ will either be merged with $R^N$, leading to the distribution of the block reward in its entirety to the consensus participants responsible for the finalization of the block for round $r$ (where $r > 12,500,000$), i.e. $R^B = R^N$, unless the duration of $R^D$ will prolonged as per decision of the community. The relevant governance procedures will be announced at a later date. The block reward distribution ratios are calculated with the following set of formulas:

$$(1)\ R^B = R^N + R^D$$

$$(2)\ R^N = R^G + R^P,$$

where $R^G$ is the Generator reward and $R^P$ is the cumulative Provisioner reward to be split amongst the participants of the three successful committees.

# 5 Concrete Parameters

Formulas introduced in Sections 5.1 and 5.2 can be considered accurate only under near-ideal network synchrony conditions. If network synchronicity drops below an abstract threshold, the outcomes of consensus liveliness and worst-case block time computations will deteriorate.

## 5.1 Consensus Liveliness

Consensus liveliness stands for the probability of the consensus not stalling for a step $s$ or a combination of steps. Below, $l$ defines the probability of liveliness during a single Provisioner committee vote:

$$l = 1 - \sum_{k=1}^{\texttt{floor}(\tau \times N)} \frac{N! \times h^k \times (1-h)^{N-k}}{k! \times (N-k)!},$$

while $p_s$ defines the probability of liveliness within a single iteration of the consensus loop for round $r$:

$$p_s = (1-h) \times l^3.$$

$n$ defines the maximum permitted number of iterations of the consensus loop, where $(1-p_s)^n \geq 2^{-100}$.

## 5.2 Worst-case Block Time

Worst-case block time is determined by setting the honesty assumption of the protocol to the lowest permissible value without violating the security of the protocol. $\Delta t$ defines the worst-case bloc

$$\Delta t = t + \sum_{j=2}^{n} (j \times t \times p_i) - ((j-1) \times t \times p_i),$$

where $p_i = (1 - p_{i-1}) \times p_s$ and $p_1 = p_s$.

The worst-case block time approaches the idealized time $t$ as the honesty assumption of the protocol approaches 1:

$$\lim_{h \to 1} (1 - \sum_{k=1}^{\texttt{floor}(\tau \times N)} \frac{N! \times h^k \times (1-h)^{N-k}}{k! \times (N-k)!}) = 1 \Longrightarrow \Delta t = t$$

### 5.3 Consensus Parameters

| Parameter | Value | Definition |
|---|---|---|
| $N$ | 64 | Committee size |
| $\tau$ | 0.67 | Threshold ratio per committee |
| $h$ | 0.75 | Node honesty ratio |
| $l$ | 0.940377 | Liveliness probability per committee |
| $p_s$ | 0.62368781434302197475 | Liveliness probability per iteration of consensus |
| $t$ | 10 | Idealized block time |
| $\Delta t$ | 20.336802914868905 | Worst-case block time |
| $n$ | 71 | Permitted iterations per consensus |
| $\mathcal{B}^{t}_{\{B^t, B^{\mathrm{floor}(t+y)}\}}$ | 3,155,760 | Number of blocks per year under idealized block time |
| $\mathcal{B}^{\Delta t}_{\{B^t, B^{\mathrm{floor}(t+y)}\}}$ | 1,559,686 | Number of blocks per year under worst-case block time |

Table 2: Consensus protocol concrete parameters

### 5.4 Economic Model Parameters

| Parameter | Value | Description |
|---|---|---|
| $b_{min}$ | 50,000 DUSK | Minimum permitted bid amount |
| $b_{max}$ | 250,000 DUSK | Maximum permitted bid amount |
| $b_{\Delta}$ | 100,000 DUSK | Assumed average bid amount |
| $s_{min}$ | 10,000 DUSK | Minimum permitted stake amount |
| $s_{max}$ | 1,000,000 DUSK | Maximum permitted stake amount |
| $s_{\Delta}$ | 100,000 DUSK | Assumed average stake amount |
| $\rho$ | 0.2 | Ratio of Generators to Provisioners |
| $r^N$ | 0.9 | Consensus participant reward ratio per block |
| $r^G$ | 0.15 | Generator reward ratio per block |
| $r^P$ | 0.00390625 | Provisioner reward ratio per block |
| $r^D$ | 0.1 | Development fund ratio per block |

Table 3: Economic model concrete parameters

## 6 ROI Estimation

ROI stands for *Return on Investment* and indicates the annual percentage of returns on an investment. In the case of Dusk Network, the ROI indicates an estimated return on the amount of DUSK being locked-up to participate in the consensus. The reader should bear in mind that the computations below do not represent a constant ROI, instead being estimations under predefined conditions. In reality, the ROI will vary depending on the number of participants, network conditions, transaction fees accrued, etc. The ROI computation does

not consider the transaction fees, meaning that in the majority of cases under the defined conditions, the realistic ROI will be higher than the respective calculation.

## 6.1 Generator

### 6.1.1 Idealized Block Time

The following formula below defines the Generator ROI under the idealized block time assumption as well as the premise that every other Generator's bid size is $\Delta b$:

$$ROI_t^G \gtrapprox \frac{\frac{b_i \times r^G \times R^B \times |\mathcal{B}^t_{\{B^t, B^{\mathtt{floor}(t+y)}\}}|}{b_\Delta \times |G|}}{b_i} = \frac{R^G \times |\mathcal{B}^t_{\{B^t, B^{\mathtt{floor}(t+y)}\}}|}{b_\Delta \times |G|},$$

where $G$ is the set of eligible Generators.

The table below outlines the expected ROIs for a predefined number of participant nodes:

| Node Type | Node Count | Block Round | Block Time | Expected ROI |
|---|---|---|---|---|
| Generator | 100 | 1-12,500,000 | $t$ | $\gtrapprox 75.74\%$ |
| Generator | 200 | 1-12,500,000 | $t$ | $\gtrapprox 37.87\%$ |
| Generator | 400 | 1-12,500,000 | $t$ | $\gtrapprox 18.93\%$ |
| Generator | 800 | 1-12,500,000 | $t$ | $\gtrapprox 9.47\%$ |

Table 4: Expected Generator ROI under idealized block time assumption

### 6.1.2 Worst-case Block Time

The following formula below defines the Generator ROI under the worst-case block time assumption as well as the premise that every other Generator's bid size is $\Delta b$:

$$ROI_{\Delta t}^G \gtrapprox \frac{R^G \times |\mathcal{B}^{\Delta t}_{\{B^t, B^{\mathtt{floor}(t+y)}\}}|}{b_\Delta \times |G|}$$

The table below outlines the expected ROIs for a predefined number of participant nodes:

| Node Type | Node Count | Block Round | Block Time | Expected ROI |
|---|---|---|---|---|
| Generator | 100 | 1-12,500,000 | $\Delta t$ | $\gtrapprox 37.43\%$ |
| Generator | 200 | 1-12,500,000 | $\Delta t$ | $\gtrapprox 18.72\%$ |
| Generator | 400 | 1-12,500,000 | $\Delta t$ | $\gtrapprox 9.36\%$ |
| Generator | 800 | 1-12,500,000 | $\Delta t$ | $\gtrapprox 4.68\%$ |

Table 5: Expected Generator ROI under worst-case block time assumption

## 6.2 Provisioner

### 6.2.1 Idealized Block Time

The following formula below defines the Provisioner ROI under the idealized block time assumption as well as the premise that every other Provisioner's stake size is $\Delta s$:

$$ROI_t^P \geq \frac{192 \times \frac{s_i \times r^P \times R^B \times |\mathcal{B}^t_{\{B^t, B^{\text{floor}(t+y)}\}}|}{s_\Delta \times |P|}}{s_i} = \frac{R^P \times |\mathcal{B}^t_{\{B^t, B^{\text{floor}(t+y)}\}}|}{s_\Delta \times |P|},$$

where $P$ is the set of eligible Provisioners.

The table below outlines the expected ROIs for a predefined number of participant nodes:

| Node Type | Node Count | Block Round | Block Time | Expected ROI |
|---|---|---|---|---|
| Provisioner | 500 | 1-12,500,000 | $t$ | $\geq 75.74\%$ |
| Provisioner | 1,000 | 1-12,500,000 | $t$ | $\geq 37.87\%$ |
| Provisioner | 2,000 | 1-12,500,000 | $t$ | $\geq 18.93\%$ |
| Provisioner | 4,000 | 1-12,500,000 | $t$ | $\geq 9.47\%$ |

Table 6: Expected Provisioner ROI under idealized block time assumption

### 6.2.2 Worst-case Block Time

The following formula below defines the Provisioner ROI under the worst-case block time assumption as well as the premise that every other Provisioner's stake size is $\Delta s$:

$$ROI^P_{\Delta t} \geq \frac{R^P \times |\mathcal{B}^{\Delta t}_{\{B^t, B^{\text{floor}(t+y)}\}}|}{s_\Delta \times |P|}$$

The table below outlines the expected ROIs for a predefined number of participant nodes:

| Node Type | Node Count | Block Round | Block Time | Expected ROI |
|---|---|---|---|---|
| Provisioner | 500 | 1-12,500,000 | $\Delta t$ | $\geq 37.43\%$ |
| Provisioner | 1,000 | 1-12,500,000 | $\Delta t$ | $\geq 18.72\%$ |
| Provisioner | 2,000 | 1-12,500,000 | $\Delta t$ | $\geq 9.36\%$ |
| Provisioner | 4,000 | 1-12,500,000 | $\Delta t$ | $\geq 4.68\%$ |

Table 7: Expected Provisioner ROI under worst-case block time assumption