DUSK

Economic Protocol Design

A deep dive into the issuance function and the gas price calculation.

POL

pol.finance

Dusk Economics

POL Finance[1] and
Emanuele Francioni[2]

[1]dipa@pol.finance, agustin@pol.finance
[2]emanuele@dusk.network

September 4, 2024

Abstract

This report presents a comprehensive proposal for designing key economic aspects of the Dusk network, focusing on token issuance, rewards distribution, and gas calculation mechanisms. These initiatives aim to enhance network security, promote sustainable growth, and ensure decentralization, while also optimizing validator participation. By employing a descending emission rate, adjusted through a variation of the well-tested half-life function, and revising the reward structure for both block generators and voters, the proposed changes seek to incentivize essential activities within the network. Additionally, the introduction of a duty-based scoring system and a predictable gas calculation process are intended to foster a dynamic and efficient blockchain environment. Supported by detailed mathematical analysis and simulations, this report outlines strategic modifications designed to significantly impact the Dusk ecosystem, aiming to improve both the economic stability and overall performance of the network.

Disclaimer

The following disclaimer is intended to clarify the purpose and limitations of the report produced by POL Finance and the Dusk Core Team for the study of the Dusk protocol. Please read this disclaimer carefully before reviewing the report.

No Financial Advice: The information provided in this report is for informational purposes only and should not be construed as financial advice, investment recommendations, or an invitation to engage in any buying, selling, or holding of any specific asset. POL Finance, Dusk Foundation and the authors do not provide financial advice, and the content of this report should not be considered as a sole or definitive source for making decisions or relying upon.

Limitation of Liability: POL Finance, Dusk Foundation and the authors assume no responsibility or liability for any financial losses, direct or indirect, incurred from using or interpreting the information provided in this report. Readers are responsible for their own investment decisions and should undertake their due diligence.

Information Obsolescence: It is crucial to acknowledge that the information provided in this report may become obsolete due to dynamic market conditions, regulatory shifts, technological advancements, or other factors. Readers should be aware that the report's content is subject to change, and it is advisable to conduct timely research and analysis before making any investment decisions.

Contents

Introduction

In the rapidly evolving landscape of blockchain technology, economic models play a crucial role in ensuring the sustainability and growth of network infrastructures. The Dusk network, recognizing the importance of a robust economic foundation, seeks to enhance its system by introducing innovative mechanisms for token issuance, distribution rewards, and gas calculation. This report presents a comprehensive analysis and proposal aimed at optimizing these critical aspects to support the network's security, sustainability, and decentralization goals.

The proposals within this report are designed to address several key challenges facing modern blockchain systems, including the incentivization of participants, efficient resource allocation, and the balancing of immediate utility with long-term value retention. Each proposal is built upon a foundation of mathematical rigor and strategic foresight, reflecting a deep understanding of blockchain economics and a commitment to the Dusk network's vision.

By exploring the nuances of token emissions, the report proposes a structured approach to issue tokens in a manner that motivates early adoption while ensuring the longevity of the network, without being exposed to possible attacks from malicious agents. Through the strategic design of reward distribution, it aims to cultivate an environment where validators and participants are fairly compensated for their contributions, enhancing network security and participant engagement. Additionally, the report delves into the complexities of gas calculation, proposing a model that aligns transaction costs with network activity, thereby fostering an efficient and cost-effective blockchain environment.

As the Dusk network continues to grow and adapt, the insights and strategies outlined in this report will serve as essential tools for navigating the challenges of blockchain economics. The proposed models are not only intended to optimize current operations but also to provide a scalable framework that can evolve in response to new technological advancements and market dynamics. This proactive approach ensures that the Dusk network remains at the forefront of blockchain innovation, offering a reliable and dynamic platform for its users.

Chapter 1

Emission design

Token emissions play a pivotal role in the early stages of a blockchain network, particularly when transaction fees alone might not be sufficient to incentivize node operators or validators. By emitting tokens over time, we can ensure that these participants are adequately rewarded for their efforts in securing and maintaining the network. This, in turn, encourages more participants to join, enhancing the network's decentralization and security.

Given the long-term vision of the Dusk ecosystem, its limited total supply, and the team's desire to reduce potential attack vectors from malicious actors, we propose to design an emission function/schedule with the following constraints:

- Total emission of 500M: A total emission of 500M DUSK ensures a controlled supply of tokens. This amount allows enough tokens to be available to reward network participants over an extended period, ensuring adequate incentives to keep the network secure and operational.

- The emission should reduce every 4 years: The model of reducing emission every 4 years has proven effective in controlling inflation and increasing token value over the long term. This approach balances the continuous issuance of new tokens with inflation control. Knowing that the emission will decrease systematically allows market actors to plan and make informed decisions.

- Total duration of 36 year: A 36-year period reflects Dusk's long-term vision, focused on building a robust and enduring network. Providing long-term incentives helps stabilize the ecosystem, minimizing the risk of sudden supply fluctuations that could destabilize the token's value and trust in the network.

- Minimize vulnerability to attacks

One of the most tested functions that accomplishes the previous constrains is the **half-life** function from Bitcoin, which is simple, easy to understand, and widely used today by protocols with a limited total supply. The basic idea is to reduce the number of tokens to be issued every certain amount of time. Actually, it is not necessarily required to reduce the emission by half like in Bitcoin, but one can use any other fraction r. Specifically, what one uses is a mathematical formula commonly known as the geometric sum:

$$\sum_{k=0}^{N} r^k = \left(\frac{1 - r^{N+1}}{1 - r} \right), \tag{1.1}$$

where $N \in \mathbb{N}$ is the number of periods. We propose designing the emission in two parts:

- **Total supply by periods:** Using the geometric sum, we can design an emission schedule for the number of periods we desire. In our case, 9 periods of 4 years.
- **Intra-period emission:** For each period, we can use either a constant or variable emission function as we deem reasonable. We will propose both approaches.

Now, if we add a term associated with the base emission (the total initial emission at the start of the schedule) denoted by E_{base}, the geometric sum becomes:

$$E_{base} \sum_{k=0}^{N} r^k = E_{base} \left(\frac{1 - r^{N+1}}{1 - r} \right), \tag{1.2}$$

and we have as much maneuverability to define this emission model as parameters in the geometric sum: the total duration in years we want the issuance schedule to last TD (Total Duration), the duration of each emission period PD (Period Duration), and the parameters E_{base}, r, N.

- N: will depend on the number of periods into which we want to partition our total schedule duration
$$N = \frac{TD}{PD} - 1.$$
The minus one is because our geometric series starts at $k = 0$.
- r: the reduction rate of the total amount of tokens we will issue in each subsequent period.
- E_{base}: once the previous parameters are defined, this base emission is defined by the closed formula of the geometric sum (1.2) with the constraint of a total supply of 500M DUSK
$$E_{base} = 500M \frac{(1 - r)}{(1 - r^9)}.$$

How to choose the above parameters?

The choice of parameters will depend on the long-term vision we have for the project. In particular, we must consider:

- **Total Duration of the Issuance Schedule (TD):** The total duration depends on the overall objective of the project and how you plan to distribute the emission over time. Here are some considerations:
  i. Project Life Expectancy: If the project has a long-term vision, a longer total duration may be suitable. If the project seeks to issue quickly to stimulate growth, a shorter duration may be better.
  ii. Network Stability: Longer durations allow for more stable and gradual growth, while shorter durations can generate greater volatility and pressure on the network.
- **Duration of Each Emission Period (PD):** The duration of each period influences the progressive reduction and predictability of the schedule. Consider the following:

i. Frequency of Emission Adjustment: Shorter periods allow for faster adjustments, while longer periods offer greater stability.

ii. Effects on Supply and Demand: The duration of the periods affects how users perceive the supply of tokens and, therefore, can influence the price and demand.

- **Reduction Factor (r):** The reduction factor r in an issuance schedule is a key parameter that determines the rate at which the emission decreases over time. For this, consider:

  i. A higher r drives faster emission, incentivizing adoption while a lower r drives slower emission to maintain stability.

  ii. If the network seeks to have a prolonged lifespan, a lower r (faster reduction) may be suitable to distribute the emission over time. For projects seeking rapid growth and requiring a constant flow of new tokens to incentivize participation, a higher r may be preferable.

  iii. The reduction factor also affects the value of the tokens and the economy of the network. A lower r can lead to a more limited supply, increasing the value of the token, while a higher r can maintain a higher supply.

Once the pace of emission for each period is defined, we can move on to define the emission within each period.

1.1 Proposal: Fixed Intra-period Emission

The simplest approach is to issue a fixed rate during each period. This is done by partitioning the total base issuance into equal parts over the number of blocks during the period. Formally, given the duration of the period PD we call PD_{blocks} the duration of the period in blocks. Lets assume we are in the k-th period, therefore $E_{base} * r^k$ is the base emission to be issued in this period. The emission function is given by:

$$f(t) \equiv \frac{E_{base} * r^k}{PD_{blocks}}, \tag{1.3}$$

where t is the block number.

Remark. Due to the fact that it is not possible to know exactly the duration of each block, the value of PD_{blocks} is in any case an estimate. However, the expected target block rate time is 10 seconds.

Pros and Cons

The advantages of this approach are

i. **Reduced Vulnerability Surface:** By employing a fixed formula for emissions, without dynamic variables that depend on manipulable network metrics, we effectively reduce the possibility of attacks or manipulations that could exploit dynamic parameters.

ii. **Stimulation of Initial Participation:** By setting a higher initial emission rate, we can foster a sense of urgency to attract early participants.

As a disadvantage, we have the fact of not using the opportunity to incentivize a desired behavior of the network, making the emission react to metrics of interest.

1.2 Emission Strategy Scenarios

To ensure the blockchain project respects a maximum total supply of 500 million tokens, we have devised three distinct emission strategies. Each strategy is tailored to stimulate early participation and secure long-term sustainability. The strategies vary by the initial emission rate (E_{base}), the rate of reduction (r), and the number of periods (N). These parameters are adjusted to ensure the total emission never exceeds the cap, following the geometric series formula (1.2). For every scenario, we are setting $N = 9$ periods of four years sustaining participant interest over a period of time of 36 years.

Scenario 1: High Initial Emission

This scenario offers the highest initial emission rate among the three. It is designed to rapidly build the user base and network participation by providing a very attractive early incentive. The reduction rate of 0.5 means the emission amount halves every period, leading to a quick decrease in available incentives after the initial burst. This can create a strong early demand but may also lead to a steep drop in incentive as the supply diminishes rapidly.

$$E_{\text{base}} = 250.48M, \quad r = 0.5$$

Scenario 2: Moderate Initial Emission

Offering a more balanced approach, this scenario provides a moderate initial emission that decreases at a slower rate compared to Scenario 1. The emission is reduced by 40% every period, balancing early high incentives with longer-term sustainability. This is designed to attract early adopters while also retaining interest and participation over a more extended period.

$$E_{\text{base}} = 201.22M, \quad r = 0.6$$

Scenario 3: Low Initial Emission

This scenario starts with the lowest initial emission and decreases at the slowest rate among the three scenarios, with a 30% reduction every period. It is the most conservative approach, offering the least initial reward but maintaining a more gradual and extended incentive distribution over time. This approach aims to build and sustain long-term growth and network participation by spreading the emission more evenly across the timeline.

$$E_{\text{base}} = 154.36M, \quad r = 0.7$$

Each of these strategies is designed to align with the project's goals of securing early engagement while managing the token economy within the constraints of a 500 million token supply cap.

Figures 1.1 illustrates the rate of token emission per period for each strategy. Scenario 1 shows a steep initial drop, reflecting a high upfront reward that decreases rapidly. Scenario 2 shows a more gradual decline, while Scenario 3 exhibits the slowest rate of decrease.

Figure 1.2 on the other hand, tracks the cumulative emission of tokens over time. It shows that Scenario 1 quickly builds up a large portion of the total emission, indicating a faster saturation. Scenario 2 accumulates at a moderate pace, and Scenario 3 progresses the slowest, preserving a larger portion of the total emission for later periods.

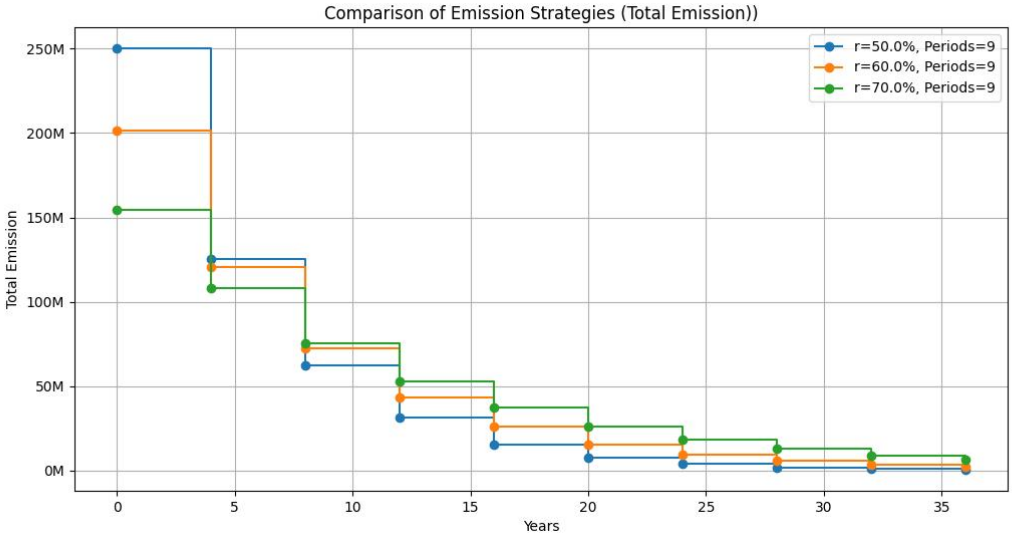

Figure 1.1: Comparison of Emission Strategies (Total Emission)

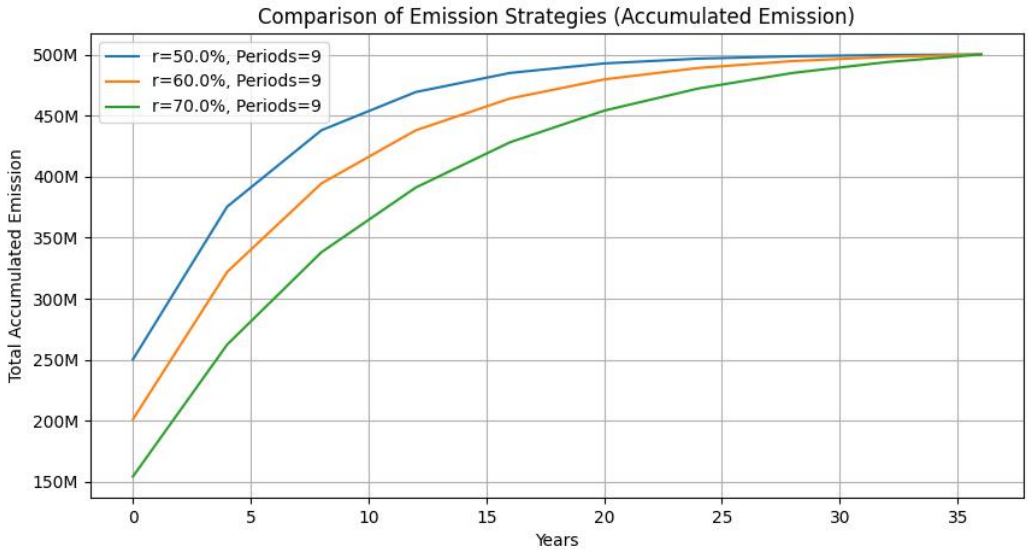

Figure 1.2: Comparison of Emission Strategies (Accumulated Emission)

Selecting $r = 0.5$ for the reduction rate in the emission strategy maximizes the initial incentive, which is crucial for encouraging high initial adoption. This approach leverages a strong early reward to attract a substantial early user base, which is fundamental in establishing a robust and decentralized network. The significant early incentive also helps in quickly building network effects, which are vital for the long-term success and sustainability of the blockchain project. This strategy effectively balances the need to stimulate

early growth with the necessity to manage the token economy within the confines of a finite supply, making it the most favorable choice among the presented scenarios.

We suggest the total duration of the schedule to be $TD = 36$ years with 9 periods of $PD = 4$ years duration, so $N = 8$. Additionally, in order to replicate Bitcoin's half-life function we would choose $r = 0.5$. Lastly, based in the formula of the geometric sum (1.2), the base emission should be $E_{base} = 250,489,236$.

To estimate block emission, we can assume a block duration of 10 seconds [1]. With this assumption, we know there will be 8,640 blocks per day, and that during the first four periods, 250,489,236 DUSK will be emitted over four years, equating to $\frac{250,489,236}{4*365} = 171,567.96$ DUSK per day. This gives us a block-by-block emission of $\frac{171,567.96}{8640} = 19.86$ DUSK.

[1] Note that if the block duration is longer, the emission schedule will be delayed accordingly, but the total emission will remain unaffected.

Chapter 2

Distribution design

The distribution of rewards on a blockchain is fundamental for incentivizing specific behaviors among the validators participating in the consensus mechanism. This incentive system is crucial for several reasons:

i. **Network Security:** Rewards motivate validators to act honestly and efficiently. By compensating them for verifying transactions and creating new blocks, it ensures that the network remains secure and resistant to malicious attacks.

ii. **Economic Sustainability:** Rewards provide an economic incentive for validators to invest in the necessary infrastructure and actively participate in the consensus process, ensuring the network's long-term sustainability.

iii. **Consensus Efficiency:** By encouraging validators to compete for rewards, it promotes quick and efficient transaction verification, which is vital for the overall performance of the blockchain.

2.1 Incentives goals

Based on a joint communication with the Dusk team and the reasons mentioned above, we will design the distribution of the rewards based on the following conditions

- The block generator shall be rewarded with a fixed coinbase plus a variable part depending on how many voters it includes in the certificate of the previous block.
  - The block generator is assigned 90% of the block emission.
  - Incentivize the block generator to include as many voters as possible by making a portion of the block reward proportional to the number of signatures in the certificate.
- Reward the voters too with a coinbase on the basis of the consensus certificates.
  - Rewards are assigned to all the voters included in the corresponding block certificate, proportionally to the number of credits of the voter in the committee.
- Consider burning (parts of) the gas spent.
- Slashing.
  - The slash amount is equal to the block reward (which varies according to the emission schedule).

– Slashing is applied to the provisioner's reward first and then to the actual stake.

Remark. Each block contains a certificate of its parent block, which contains the votes of all validators that agreed on such block.

2.2 Distribution Updates

Based on the aforementioned objectives, and considering that the emission schedule is already predefined, we propose modifying the rewards distribution part as follows:

- 80% to the block generator (proposal step)
- 5% to the validation committee (validation step)
- 5% to the ratification committee (ratification step)

This way, we incentivize each step of the SA consensus process, giving higher priority to the block generator, which we consider the most important step.

Furthermore, to encourage the block generator to include as many voters in the certificate as possible, we propose that the percentage of the total reward they receive also depends on the number of votes obtained in the Validation and Ratification steps. Distributing 90% to the block generator, a proposal is

$$generator_{reward} = \begin{cases} 0 & \text{if } C_f < 0.67 \\ 80\% \times Total_{reward} \times \left(w_{\text{Proposal}} + \frac{(C_f - 0.67)}{0.33} \times (1 - w_{\text{Proposal}}) \right) & \text{otherwise} \end{cases}$$

$$voter_{reward} = \begin{cases} 0 & \text{if } V_f < 0.67 \\ 5\% \times Total_{reward} \times \frac{(V_f - 0.67)}{0.33} & \text{otherwise} \end{cases}$$

where

- $C_f = \frac{\#\ certificate\ credits\ used}{\#\ total\ committee\ credits}$, $V_f = \frac{\#\ voter's\ credits}{\#\ total\ committee\ credits}$ are the percentage of credits included in the certificate by the generator and the voter resp.;
- $Total_{reward}$ is the total emission of the block plus the gas fee;
- $0 < w_{Proposal} \leq 1$ is a weight that controls how much predominance we want to assign to the part of the number of favorable votes in the certificate;
- *# certificate credits used* is the total number of credits included in the block certificate and *# voter's credits used* is the number of credits of the voter in the committee;
- *# total committee credits* $= 128$ are the total credits distributed.

The formula was designed in order that

- **Threshold (67%):** Rewards are only paid if at least 67% of the credits are used. This ensures that participants are incentivized to use a significant majority of the credits before receiving rewards.

- **Incremental Reward:** Rewards increase proportionally to the percentage of credits used above 67%, up to a maximum of 100%. This further incentivizes the complete use of available credits.

Burning mechanism:

Lastly, regarding the burning of gas, we propose burning all the gas that has not been successfully distributed

$$80\% \times Total_{reward} \times \left(1 - \frac{\#\ committee\ credits\ used}{\#\ total\ committee\ credits}\right)(1 - w_{Proposal}) + 2 * 5\% \times Total_{reward} * \frac{\#\ total\ credits\ not\ used}{\#\ total\ committee\ credits}$$

2.2.1 Improvements

Incentivizing the Inclusion of Votes in the Certificate

The strategy of making the block generator's reward dependent on the number of votes included in the certificate aims to foster greater participation and security in consensus. However, it's crucial that this mechanism doesn't allow for easy manipulation or gaming of the system. For this purpose, introducing a minimum threshold of votes required for the block generator to qualify for the variable portion of the reward can ensure that the incentive for including more voters activates only after achieving significant and representative participation.

Gas Burning as an Adjustment Mechanism

The idea of burning a part of the spent gas positively contributes to the healthy evolution of the DUSK token, as it can help adjust the currency supply and potentially increase its value. However, this mechanism must be carefully balanced to not disincentivize participation due to high transaction costs.

Bonuses for Efficiency and Security

To adapt to long-term changes in network behavior and the economy, the emission schedule could include adjustment mechanisms that allow modifications based on key indicators of network health and security. This could take the form of periodic adjustments in reward proportions based on assessments of the network's efficiency, participation, and security. For instance, in certain ranges of network efficiency, the emission could be increased to boost the rewards distributed among agents, without exceeding the maximum limit per block.

2.2.2 Scenario Analysis

We consider three possible states of committee credits used and voters participation, varying between low, medium, and high, resp. These refers to the total number of credits included in the block certificate by the generator and the proportion of active voters in the committee voting agreement process.

The percentage of committee credits used and voters participation are chosen as

- Low: A committee credits used and voters participation between 67% and 78%.
- Medium: A committee credits used voters participation between 78% and 89%.
- High: A committee credits used and voters participation between 89% and 100%.

The daily emission is based on the high initial emission scenario described in the previous chapter

$$\frac{250.24M}{4 * 365}.$$

It is important to note that the rewards received by the generator are determined by a fixed percentage of the emission ($w_{Proposal}$) and a variable one that depends on the proportion of the certificate credits used, as seen in the generator reward equation. On the other hand, the rewards received by the voters depend on the proportion of active voters in the committee voting agreement process. Finally, the remainder is burned. This reward structure aims to incentivize greater participation and an effective consensus process in the DUSK network.

We will show the output for the following combination of the percentage of issued tokens distributed to the block generator vs $w_{Proposal}$

- Percentage for the block generator of 90% and $w_{Proposal}$ is set at 70%, Figure 2.1.
- Percentage for the block generator of 90% and $w_{Proposal}$ is set at 60%, Figure 2.2.
- Percentage for the block generator of 80% and $w_{Proposal}$ is set at 70%, Figure 2.3.
- Percentage for the block generator of 80% and $w_{Proposal}$ is set at 60%, Figure 2.4.

For robustness, we have used 25 different seeds in order to cover distinct random cases. The plots are the result of using the average of all runs.

In our analysis, we compare the dynamics of rewards for the generator, voters, and burned Dusk for the scenarios of generator and voters participation in low, medium, and high states, as shown in the Figures 2.1-2.4. We observe that when both the emission and voting are high, the generator and voters receive higher rewards, resulting in a lower amount of burned Dusk. On the other hand, when both participation percentages are low, a significant portion of the tokens are burnt. Note that when the fixed amount given by $w_{Proposal}$ is set at 60%, burned tokens have a higher impact in the total issuance.

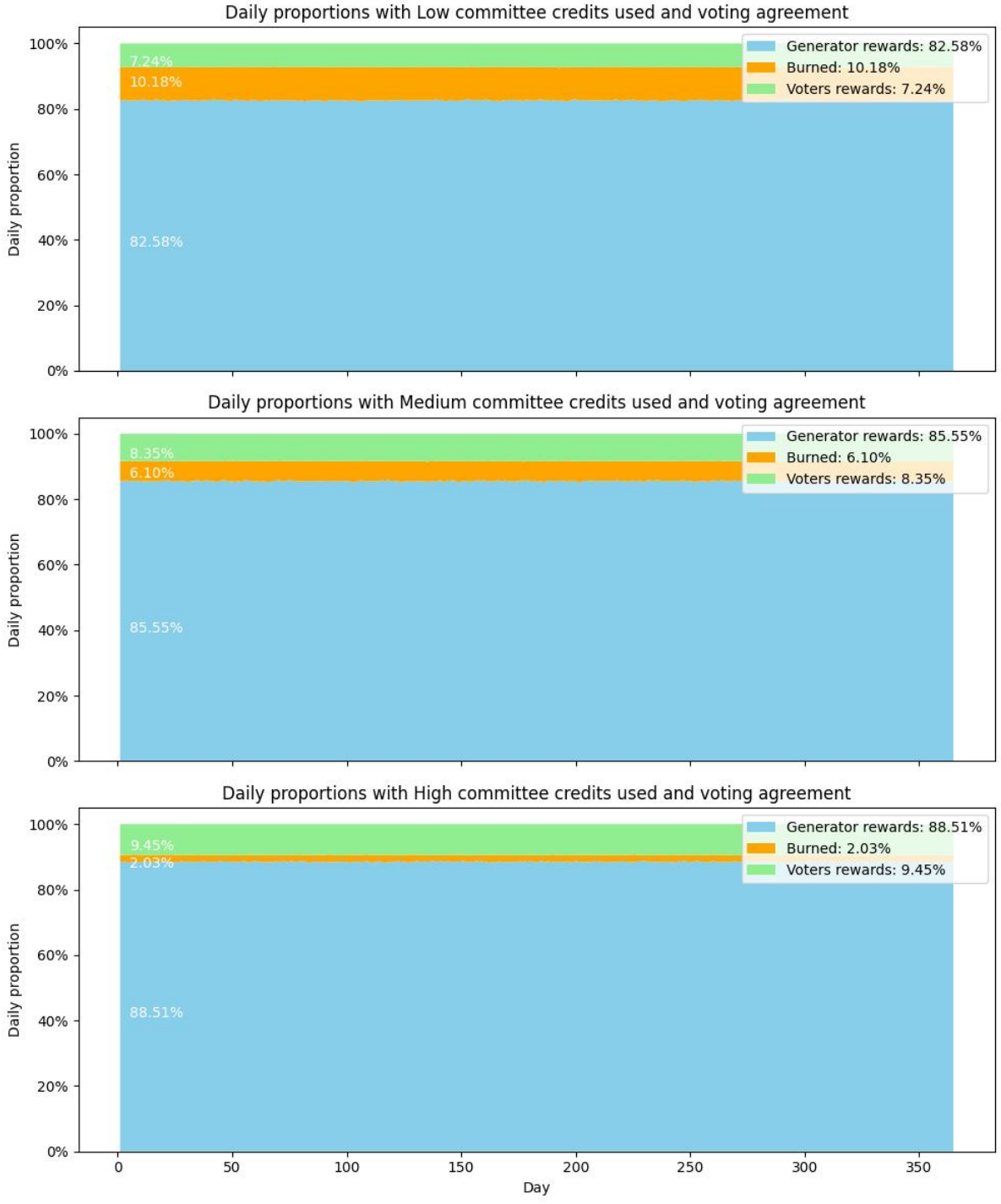

Figure 2.1: Dynamics of reward percentages for different daily emission (90% to block generator with 70% fixed).

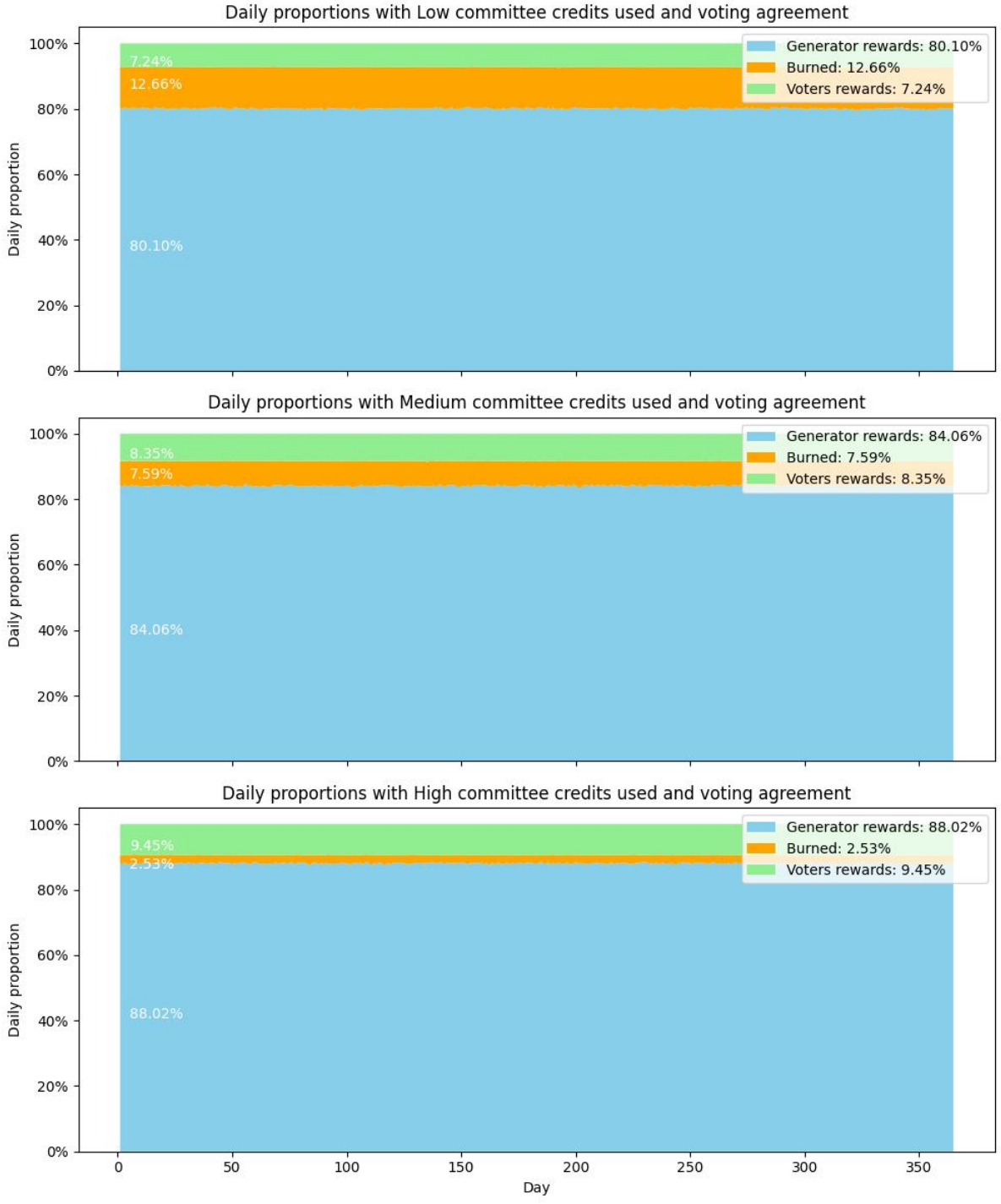

Figure 2.2: Dynamics of reward percentages for different daily emission (90% to block generator with 60% fixed).

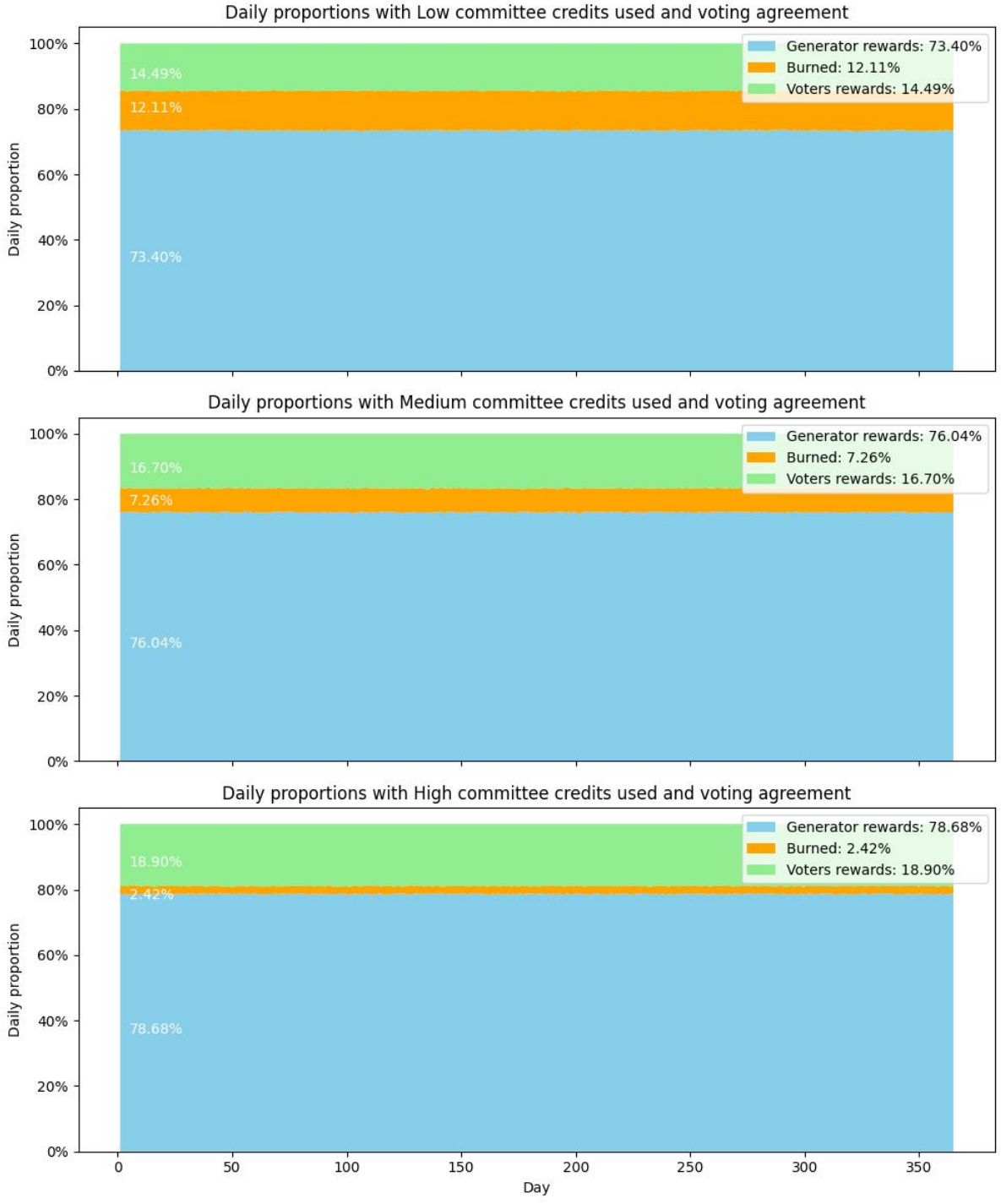

Figure 2.3: Dynamics of reward percentages for different daily emission (80% to block generator with 70% fixed).

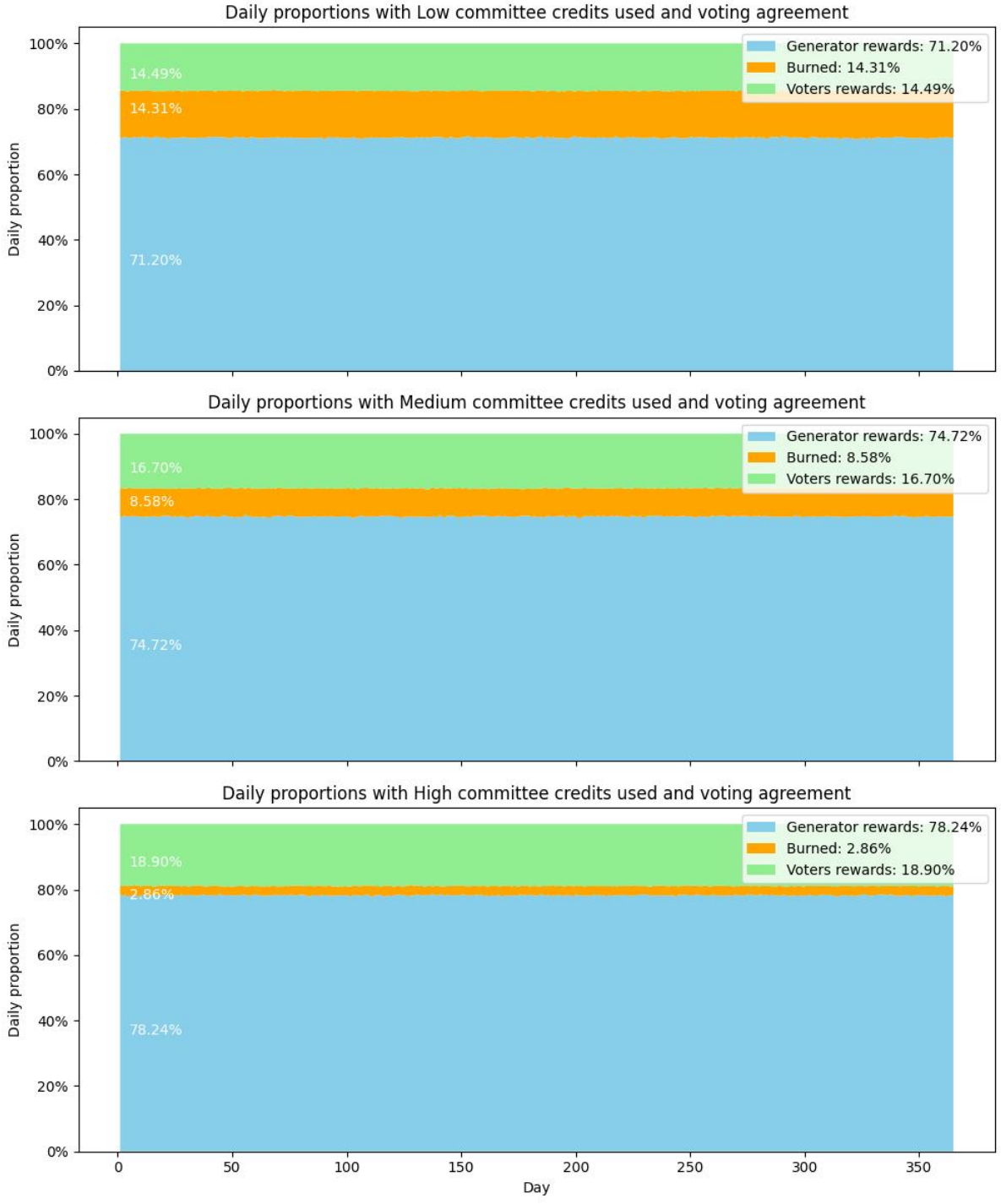

Figure 2.4: Dynamics of reward percentages for different daily emission (80% to block generator with 60% fixed).

Chapter 3

Gas calculation design

In the context of the Dusk and its economic protocol, gas is a fundamental concept central to the execution and processing of transactions on the blockchain. Gas can be thought of as the fuel that powers blockchain operations, similar to how gasoline powers a vehicle.

Gas is used as a unit of measure to allocate resources on the blockchain. Each operation, whether it's a simple transaction or a complex smart contract execution, requires a certain amount of computational power and storage. Gas quantifies this resource usage and it is of paramount importance having a precise mechanism that aligns the price of each unit of gas with the available resources in the chain.

3.1 Gas price calculation

The economic protocol (here) includes novel mechanisms to let smart contracts pay for gas. In that respect, it is important to develop some best practices to let developers come up with a way to let the smart contracts set the gas price dynamically and what parameters would Dusk need to provide the smart contracts with (e.g. moving average of gas price per epoch, average gas price last block, etc).

Gas inputs

The EIP-1559 model introduces an innovative mechanism for fee management in Ethereum, enhancing cost predictability and aiming to align gas prices with the actual network conditions. If we aim to design a system that allows a smart contract to suggest a gas price, incorporating additional market signals, here are some ideas that could be tailored to these requirements:

i. **Feedback from Network State**: Implement a mechanism that adjusts the price suggestion based on the current state of network congestion, similar to the base price adjustment in EIP-1559.

ii. **Using Moving Averages**: Employ the moving average of gas prices from recent blocks to smooth out short-term fluctuations and provide a more stable estimate of the gas price the smart contract should propose. This approach could be implemented using Simple Moving Average (SMA) which calculates the average gas price of the last N blocks. It's simple and effective for capturing a general trend, but may be reactive to sudden changes.

To implement any of these strategies, access to reliable and up-to-date data on network state and transactions is crucial. This could be achieved through oracles providing

the smart contract with the necessary information to calculate the suggested gas price. Additionally, it's important to consider the additional cost and complexity that these implementations might introduce, both for the development of the smart contract and its execution on the network.

3.1.1 Proposal

To integrate the two previous points and give greater emphasis to the automatic feedback proposed by EIP-1559, we can design a formula that incorporates these elements in a weighted manner. The goal is to create an adaptive mechanism that considers the gas price trend (through moving averages), immediate information from the last block, and a dynamic adjustment based on network congestion. The formula could look as follows:

$$\begin{aligned}\text{Suggested Gas Price} = w_1 \cdot \text{Base Price EIP-1559} \\ + w_2 \cdot \text{Moving Average}\end{aligned}$$

where:

- Base Price EIP-1559 is the current base price according to the EIP-1559 mechanism:

  $$\text{New Base Price} = \text{Previous Base Price} \times \left(1 + \frac{\text{Used Capacity} - \text{Target Capacity}}{\text{Target Capacity}}\right),$$

  where Target Capacity = 50%.

- Moving Average is simple moving average of gas prices from the last N blocks

  $$SMA = \frac{P_1 + P_2 + \cdots + P_N}{N}.$$

  We suggest using an N large enough to cover a significant number of past blocks, but without excessively increasing the required computational power. One third of the total daily blocks sounds reasonable. Assuming a block takes about 10s to complete, we propose $N = 2880$.

- w_1 and w_2 are the weights assigned to each of these factors, where $w_2 = 1 - w_1$.

We could assign the weights as follows: $w_1 = 0.5$ (50%), $w_2 = 0.5$ (50%). These weights are considered as an initial starting point and could be adjusted based on the algorithm's performance in practice. This choice of weights is also supported by the sensitivity analysis conducted, detailed in Section 3.1.2.

Additional Considerations: This model assumes that the smart contract has access to these data in real-time, in order to have information on gas prices and current network congestion. Furthermore, it is crucial to monitor and adjust the weights as needed to maintain the desired balance between stability and responsiveness to market conditions.

This weighted sum is a theoretical model, and its effective implementation would depend on a careful evaluation of its behavior in the specific blockchain network environment, as well as gas optimization considerations for the execution of the smart contract itself.

Finally, note that instead of using a weighted sum another approach is to adjust the amount of blocks N used in the calculation of the SMA. The problem with this, although it could adjust quickly to changes in the congestion, is that the formula will lost the impact that EIP-1559 has on network demand when varying the base fee based on network congestion.

3.1.2 Analysis of Weight Sensitivity

Next, we will evaluate the behavior of the output from the new proposal for base fee calculation by analyzing the base fee itself along with two other metrics associated with volatility:

- Average Moving Amplitude (AMA): This calculates the amplitude (difference between the maximum and minimum) of gas prices within a moving window (e.g., daily or weekly). The average of these amplitudes over time can serve as an intuitive measure of volatility.
- Interquartile Range (IQR): The IQR measures the spread of the middle half of your data (between the first and third quartile) and can give you an idea of the variability of gas prices, minimizing the effect of extreme outlier values.

We have simulated one year assuming

- A network congestion and voter participation level of medium.
- An initial base fee of 1 LUX.
- A target gas capacity used of 50% for the EIP-1559 term.

In the same sense that for the issuance analysis, we have used 25 different seeds in order to cover distinct random cases.

General Analysis

The proposed weight combinations for calculating the base fee show significant variations in terms of volatility and response to market conditions. Comparing these scenarios reveals crucial differences in how each configuration handles stability and adaptability to market fluctuations.

We consider a medium congestion scenario for the analysis of the weights, as in low and high congestion, the base fee price is decreasing and increasing (at an exponential rate) respectively, causing the price to tend towards zero or rise indefinitely. It is unrealistic to assume that these extreme scenarios remain constant over time. Therefore, it is sufficient to consider a medium congestion scenario to compare the impact of weight sensitivity.

Base Fee: In Figure 3.1, we observe that the configuration with a higher weight towards EIP-1559 (90% EIP-1559, 10% SMA) introduces greater flexibility, allowing for quicker adjustments to market conditions but with the risk of increased volatility. On the other hand, increasing the weight of SMA (up to 90% SMA, 10% EIP-1559) shows a tendency to maintain a more stable base fee, though potentially less responsive to sudden market changes.

AMA (Amplitude Moving Average): A higher weight towards EIP-1559 increases the sensitivity of the AMA, highlighting greater adaptability but also potentially unwanted volatility, as seen in Figure 3.2. The balanced configuration (50% EIP-1559, 50% SMA) appears to offer a compromise between stability and adaptability.

IQR (Interquartile Range): Lastly, the IQR provides a robust measure of central dispersion, minimizing the impact of outliers. In Figure 3.3, we observe how the trends here follow similar patterns to those of the AMA, with configurations more inclined towards SMA favoring stability. The three cases seem similar due to the utilization of 25 different seeds, which helps to eliminate outliers as we showed the average behaviour.

Conclusion

Considering the goal of balancing robustness, dynamism, and smoothness in adapting to market changes, the configuration **50% EIP-1559, 50% SMA** emerges as the most balanced option. This approach provides an optimal blend of EIP-1559's adaptability and the inherent stability of SMA, allowing for more precise adjustments without falling into excessive reactions to minor fluctuations. This configuration promotes a predictable experience for users while maintaining the system's ability to adapt to significant demand variations.

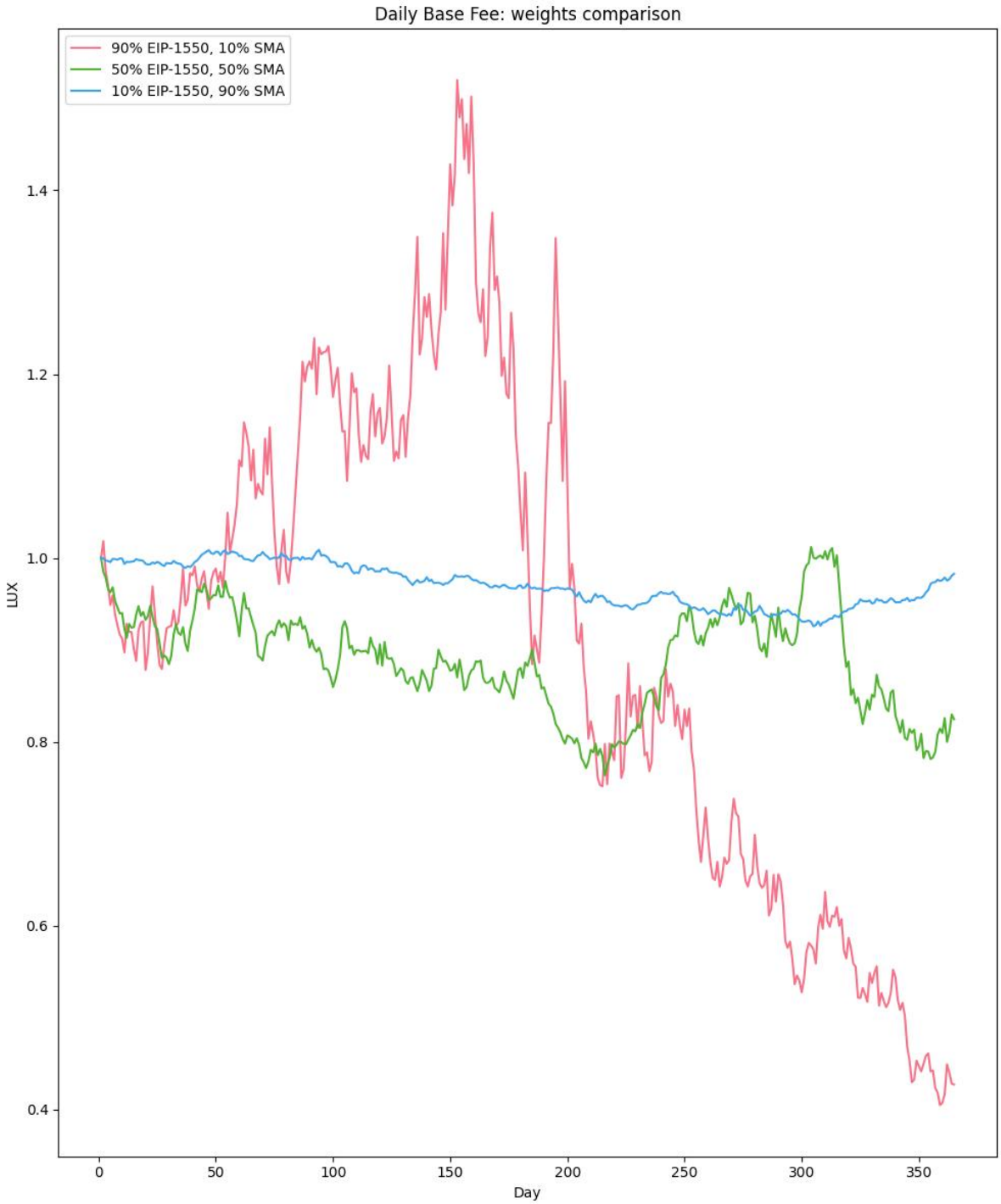

Figure 3.1: Base Fee Weights Comparison

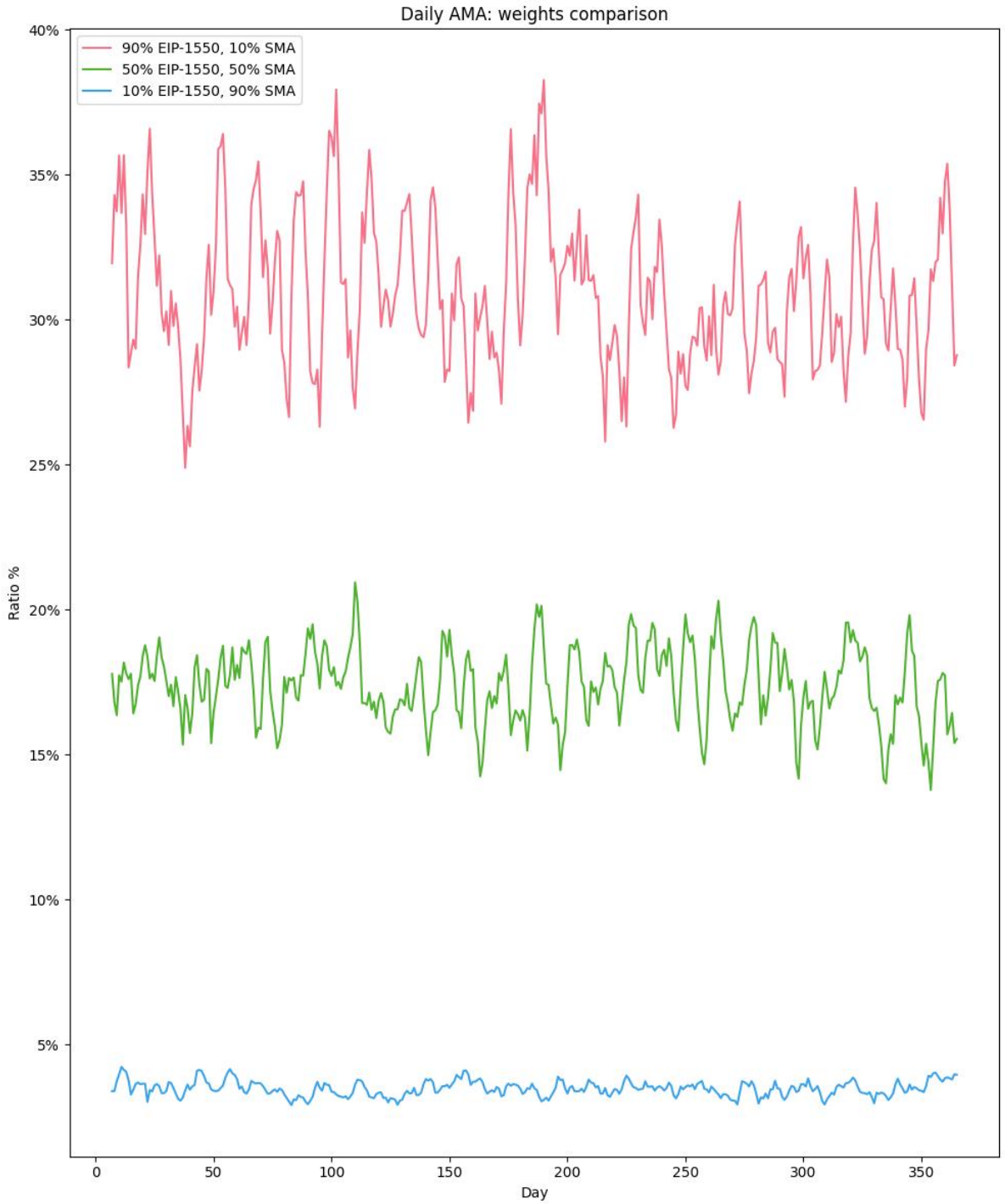

Figure 3.2: AMA Weights Comparison

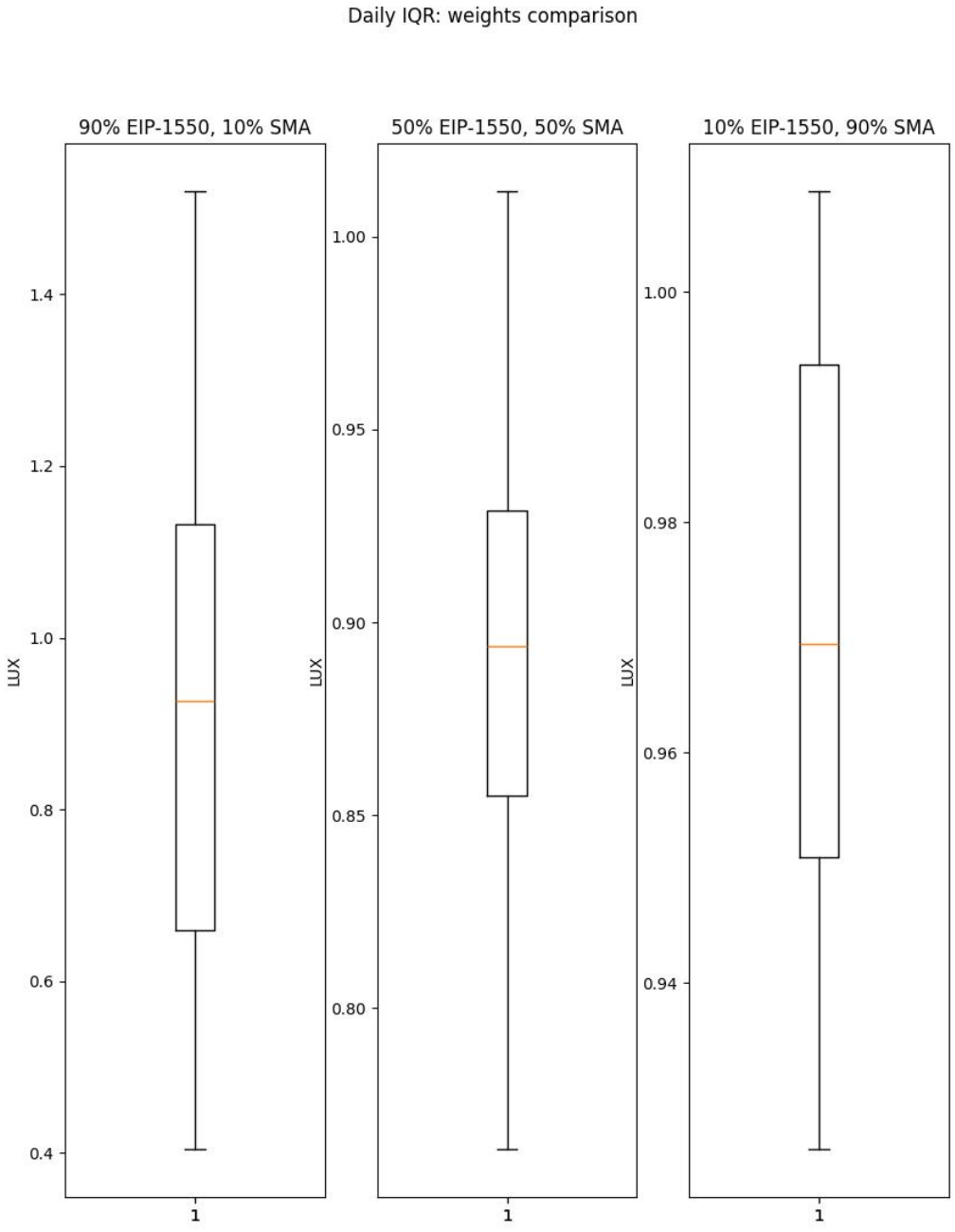

Figure 3.3: IQR Weights Comparison

Conclusion

This report has outlined comprehensive strategies and proposals aimed at optimizing the economic mechanisms underlying the Dusk network, ensuring its long-term sustainability, security, and decentralization. By adopting a methodical approach to emission, distribution, and gas price calculation, this framework is designed to foster a robust and thriving blockchain ecosystem.

The proposed emission strategies minimize vulnerability to attacks while balancing the need for immediate incentivization with long-term viability, ensuring the Dusk network can attract and sustain a diverse group of participants. By implementing a geometric sum approach with variable reduction rates, the project can adjust token supply dynamically, ensuring alignment with network growth and token value stability.

In the realm of distribution, the updated reward structure is tailored to promote fairness and efficiency among validators and participants. The introduction of a duty-based scoring system incentivizes critical behaviors that enhance network integrity and performance. This system not only rewards participation but also encourages active and meaningful engagement in the consensus process.

The gas price calculation design integrates innovative elements from the EIP-1559 model, enhancing predictability and aligning gas costs with network demand. This approach is critical in maintaining network efficiency and ensuring that transaction costs remain fair and proportional to the actual computational effort required.

Overall, these strategies demonstrate a forward-thinking approach to blockchain economics, one that leverages detailed mathematical modeling and strategic insights to craft policies that are both effective and equitable. As the Dusk network continues to evolve, these proposals will provide a foundation for responsive and adaptive management, ensuring that the network remains competitive and compliant with the shifting landscapes of blockchain technology and market demands.

By continuing to refine and implement these strategies, Dusk can achieve its goal of creating a decentralized platform that not only meets the current demands of its users but also anticipates future challenges and opportunities in the blockchain space.

Appendix A

Analysis on Bell-shaped emission

In this section we will analyze a novel approach resembling a normal distribution, where the emission peaks at a certain point in the future and then decreases. This design not only stimulates initial participation but also retains significant incentives for future adoption.

A.1 Mathematical Design

We define the emission using a normal distribution, characterized by its mean (μ) and standard deviation (σ), which determine the peak emission point and the spread of the distribution, respectively. The emission schedule can be described as follows:

$$f(x) = \frac{1}{\sqrt{2\pi\sigma^2}} e^{-\frac{(x-\mu)^2}{2\sigma^2}} \tag{A.1}$$

where:

- μ is the mean, the point in time where the emission is highest.
- σ is the standard deviation, controlling the spread of the distribution.

A.2 Discrete Emission Periods

The total duration is divided into periods of 4 years each, resulting in 9 periods ($N = 9$). The emission for each period is calculated by integrating the normal distribution over the period and normalizing the total supply to 500 million tokens.

A.2.1 Calculating Emissions

Given the total supply E_{total}, the emission for each period is calculated using the following steps:

- Normalize the distribution to ensure the total emission is 500M tokens.
- Calculate the fraction of tokens emitted in each period.
- Accumulate emissions over time to ensure total supply does not exceed 500M.

The emission for each period is determined by:

$$E_i = E_{total} \cdot \frac{f(i \cdot PD)}{\sum_{k=0}^{N} f(k \cdot PD)} \tag{A.2}$$

where PD is the period duration (4 years).

A.2.2 Emission Schedule

Here, we present the parameters used in our model:

- **Total Supply** (E_{total}): 500M tokens
- **Duration** (TD): 36 years
- **Period Duration** (PD): 4 years
- **Mean** (μ): 18 years (point of peak emission)
- **Standard Deviation** (σ): 6 years (spread of the emission)

Using these parameters, we calculate the emission for each period by integrating the normal distribution and ensuring the total emission aligns with the 500 million tokens cap. The following figures illustrate the emission schedule and the total accumulated emission over time.

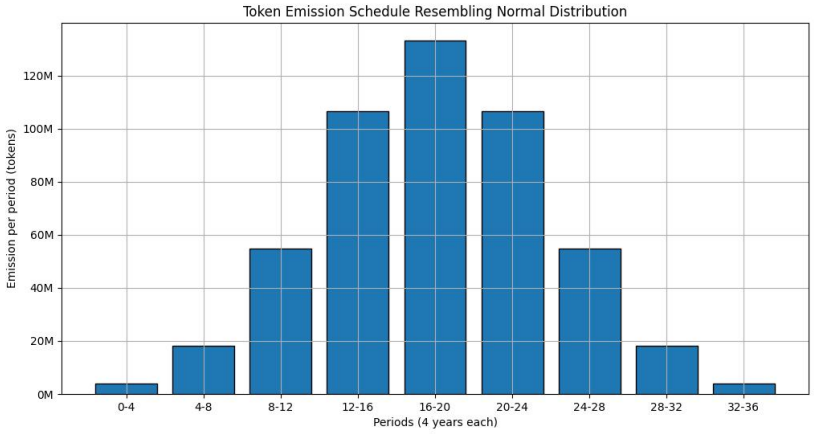

Figure A.1: Token Emission Schedule Resembling Normal Distribution

Observation: This figure shows the emission per period, with the highest emission occurring around the 16-20 year mark, followed by a gradual decline.

Observation: This figure illustrates the total accumulated emission over time. The emission accumulates rapidly around the midpoint, reflecting the peak emission period, and then tapers off towards the end of the 36-year duration.

These visuals provide a clear understanding of how the token emission is distributed over time and serve as a foundation for comparing different scenarios to optimize for various objectives, such as early adoption incentives (FOMO) and long-term sustainability.

A.3 Advantages and Disadvantages of Normal Distribution Approach

The advantages of this approach are

i. *Sustainability*: Maintains significant incentives for both early and later participants, promoting long-term engagement.

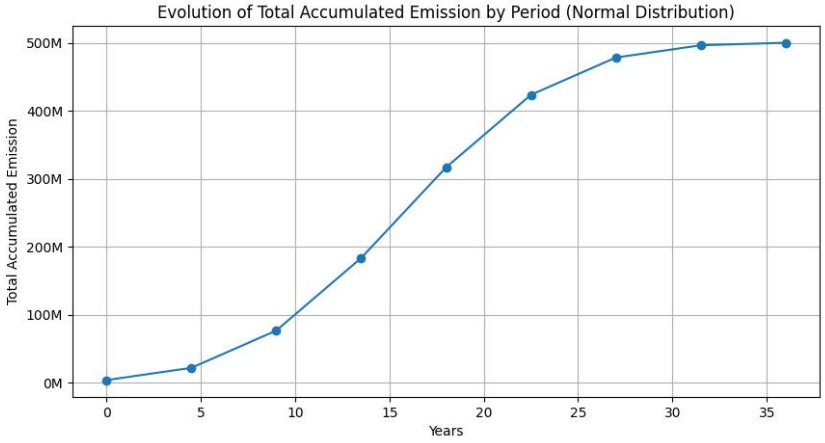

Figure A.2: Total Accumulated Emission by Period (Normal Distribution)

ii. *Balanced Growth*: Reduces the risk of rapid value depreciation by spreading emissions over a longer period.

As disadvantages we can mention

i. *Sensitivity*: More susceptible to token price fluctuations due to the anticipated significant increase in supply in the near future. In the event of an upward price trend, the benefits would be minimal. However, in the event of a downward trend, the perceived increase in supply would exacerbate selling pressure.

ii. *Complexity*: More complex to implement and communicate compared to a simple half-life model.

iii. *Initial Interest*: Lower initial emissions might not generate enough early interest.

A.4 Emission Strategy Scenarios

To ensure the blockchain project respects a maximum total supply of 500 million tokens, we have devised three distinct emission strategies. Each strategy is tailored to stimulate early participation and secure long-term sustainability. The strategies vary by the period duration (PD), the mean (μ), and the standard deviation (σ). These parameters are adjusted to ensure the total emission never exceeds the cap, following the normal distribution model. For each scenario, we are setting a total duration of 36 years, $\mu = 18$ year and $\sigma = 6$ years.

Scenario 1: Short Period Duration for High Initial FOMO

This scenario uses shorter periods of 2 years each to provide a higher frequency of token emission adjustments. This results in a more aggressive initial emission, aimed at maximizing early adoption incentives.

$$PD = 2 \text{ years}, \quad \mu = 18 \text{ years}, \quad \sigma = 6 \text{ years}$$

Scenario 2: Standard Period Duration for Balanced Incentives

Here, we maintain the standard period duration of 4 years. This provides a balanced approach, offering moderate initial incentives and ensuring a steady emission rate over time.

$$PD = 4 \text{ years}, \quad \mu = 18 \text{ years}, \quad \sigma = 6 \text{ years}$$

Scenario 3: Long Period Duration for Sustained Incentives

This scenario uses longer periods of 6 years each. It aims to reduce the frequency of emission adjustments, spreading out incentives over a longer duration to promote sustained network participation and stability.

$$PD = 6 \text{ years}, \quad \mu = 18 \text{ years}, \quad \sigma = 6 \text{ years}$$

Each of these strategies is designed to align with the project's goals of securing early engagement while managing the token economy within the constraints of a 500 million token supply cap.

Figure A.3 illustrates the rate of token emission per period for each strategy. Scenario 1 shows a rapid emission increase with frequent adjustments, Scenario 2 presents a more gradual emission pattern, and Scenario 3 exhibits the slowest rate of increase, reflecting sustained incentives over a longer period.

Figure A.4 tracks the cumulative emission of tokens over time. Scenario 1 quickly accumulates a large portion of the total emission, indicating faster saturation. Scenario 2 accumulates at a moderate pace, while Scenario 3 progresses the slowest, preserving a larger portion of the total emission for later periods.

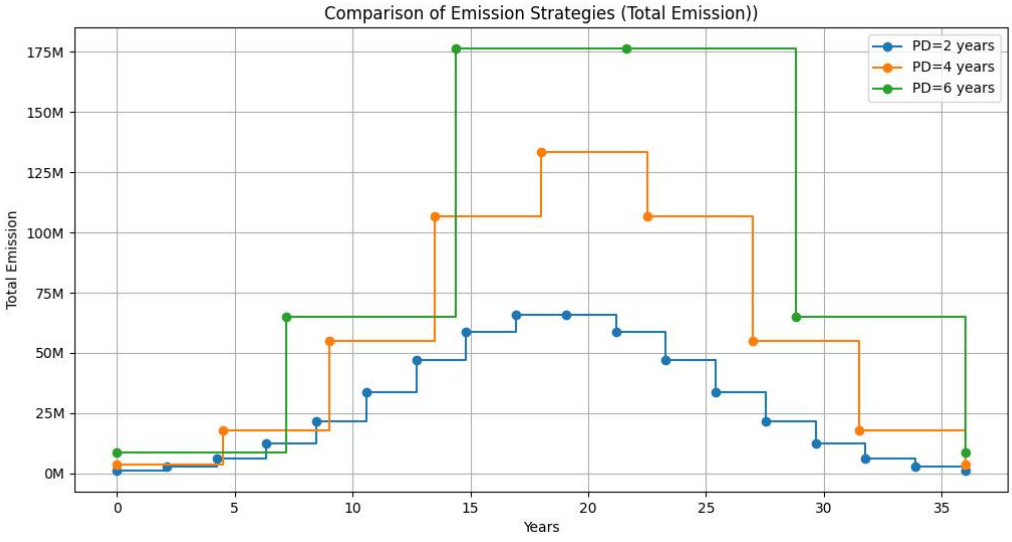

Figure A.3: Comparison of Emission Strategies (Total Emission)

Selecting a shorter period duration for the emission strategy maximizes the initial incentive, which is crucial for encouraging high initial adoption. This approach leverages a strong early reward to attract a substantial early user base, fundamental for establishing a robust and decentralized network. The significant early incentive also helps in quickly

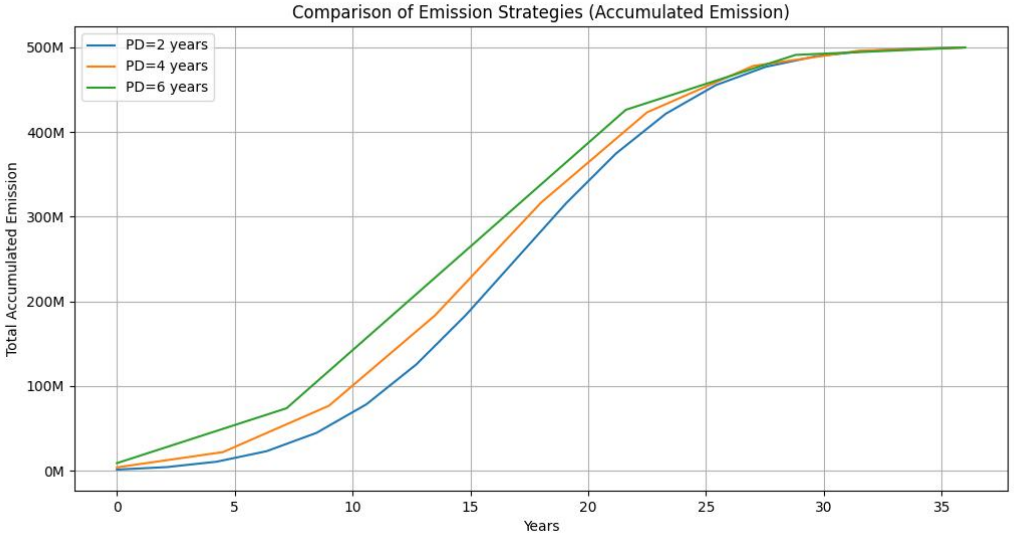

Figure A.4: Comparison of Emission Strategies (Accumulated Emission)

building network effects, which are vital for the long-term success and sustainability of the blockchain project. This strategy effectively balances the need to stimulate early growth with the necessity to manage the token economy within the confines of a finite supply, making it a favorable choice among the presented scenarios.

A.5 Conclusion

While theoretically unproblematic, the bell-shaped variation would be a more risky approach. We propose utilizing the half-life function, as it is empirically validated by numerous protocols, minimizes potential attacks and manipulations, and does not exhibit the sensitivity to price fluctuations mentioned in the previous disadvantages.

Appendix B

Provisioner APR

To accurately estimate the APR, it is essential to consider the token issuance, distributed rewards, and the total amount of tokens staked.

The total issuance of DUSK is designed to decrease every four years, following a geometric sum function. This reduction directly affects the number of tokens available for distribution as rewards to the provisioners. We will illustrate the evolution of the APR for a provisioner, assuming a total supply of 500M tokens.

In this system, , the block reward should be partitioned as 10% to Dusk Development Fund, 10% to voters, and 70% fixed with an extra 10% conditional on the addition of extra votes. Moreover, the burning of gas fees can influence the final rewards received by the provisioners.

To analyze this, we simulate different scenarios considering the total network stake and the stake of the provisioner node. We will calculate the best case scenario in which the provisioner receives 128 credits and includes all votes. The APR is defined as:

$$APR = \frac{Provisioner_{Total\_Reward}}{\text{Stake of the node}} \tag{B.1}$$

where $Provisioner_{Total\_Reward}$ are the annual earnings.

To calculate these earnings, we will estimate the amount of DUSK issued in each block over the course of one year using the Scenario 1 from section 1.2. We will assume that each block takes 10 seconds [1] to be created. Based on the provisioner's participation percentage, we will assign a role as generator or voter and calculate the rewards received according to the formulas in section 2.2.

The rewards received in each role are summed and distributed based on the proportion of the node's stake relative to the total network stake:

$$Provisioner_{Total\_Reward} = (generator_{reward} + voter_{reward}) \times \frac{\text{Stake of the node}}{\text{Total network stake}}$$

Since the provisioner can be chosen as either a generator or a voter in each block, the total rewards at the end of the year will be the sum of the rewards received in each of these roles.

Assuming a total supply of 500M tokens we explore different scenarios. We consider three node's stake representing 5%, 10% and 20% of the total network stake. For each scenario we will vary the total stake of the network and we will provide a plot of the APR received.

[1] This duration is currently enforced by the protocol as blocks cannot be generated before 10 seconds after the previous block.

It is important to note that in scenarios where the total network stake is lower, the APR is higher. This is because, as the total network stake increases, the absolute amount of the node's stake also increases (since it always represents 10% of the total), leading to a higher total investment. However, the rewards received remain constant.

Figure B.1 depicts the evolution of the APR as a function of the stake invested by the node for all the scenarios.

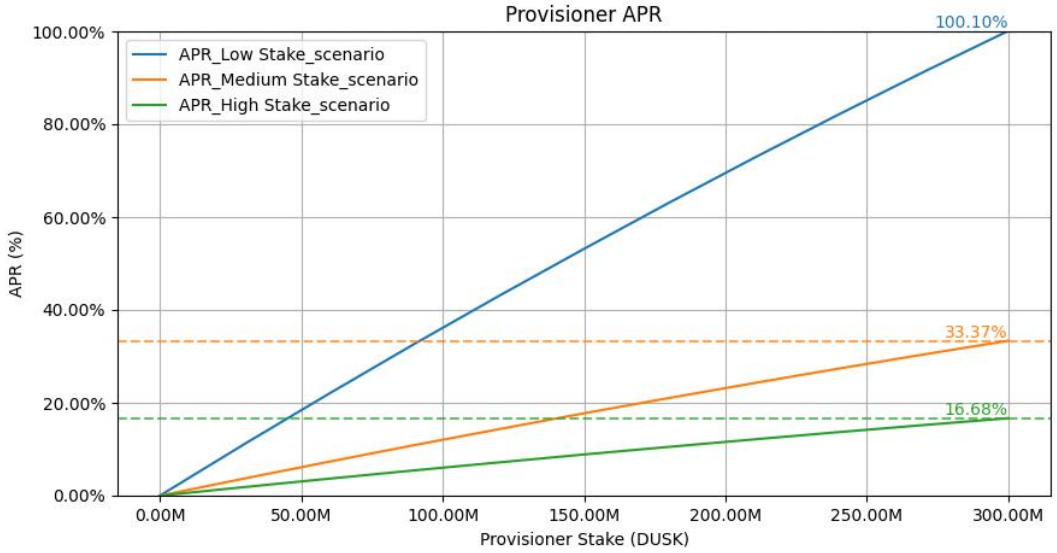

Figure B.1: Provisioner APR for each scenario

Figure B.2 depicts the evolution of the APR as a function of the total stake of the network.

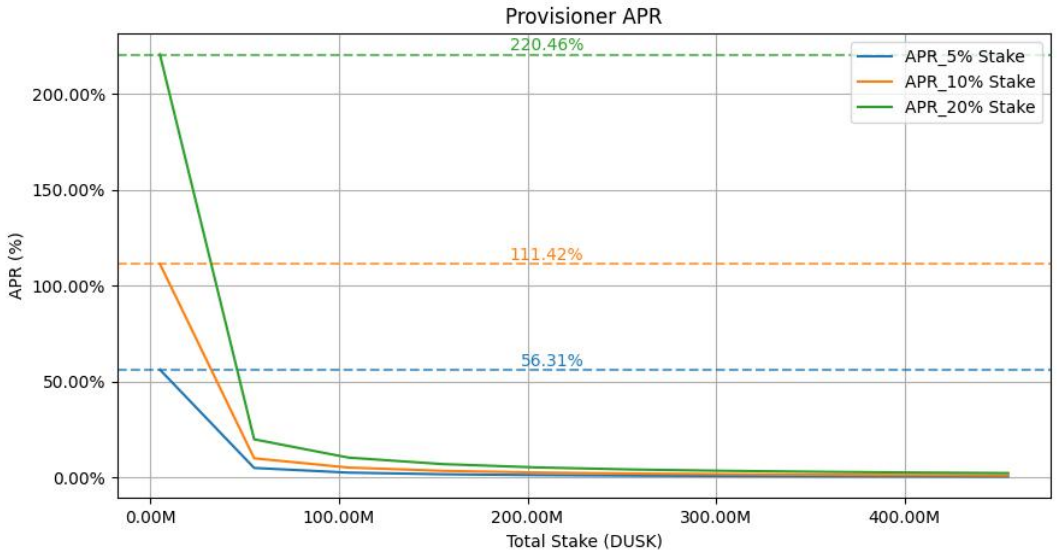

Figure B.2: Provisioner APR for each scenario

For example, suppose the total network stake is 10% of the total supply, meaning the total stake is 50M DUSK. If the provisioner decides to stake 20% of that, that is 10M

DUSK, then by the end of the year he will earn 2198668 DUSK. Using (B.1) he will obtain earnings of approximately

$$APR = \frac{2198668}{10M} \simeq 22\%.$$