

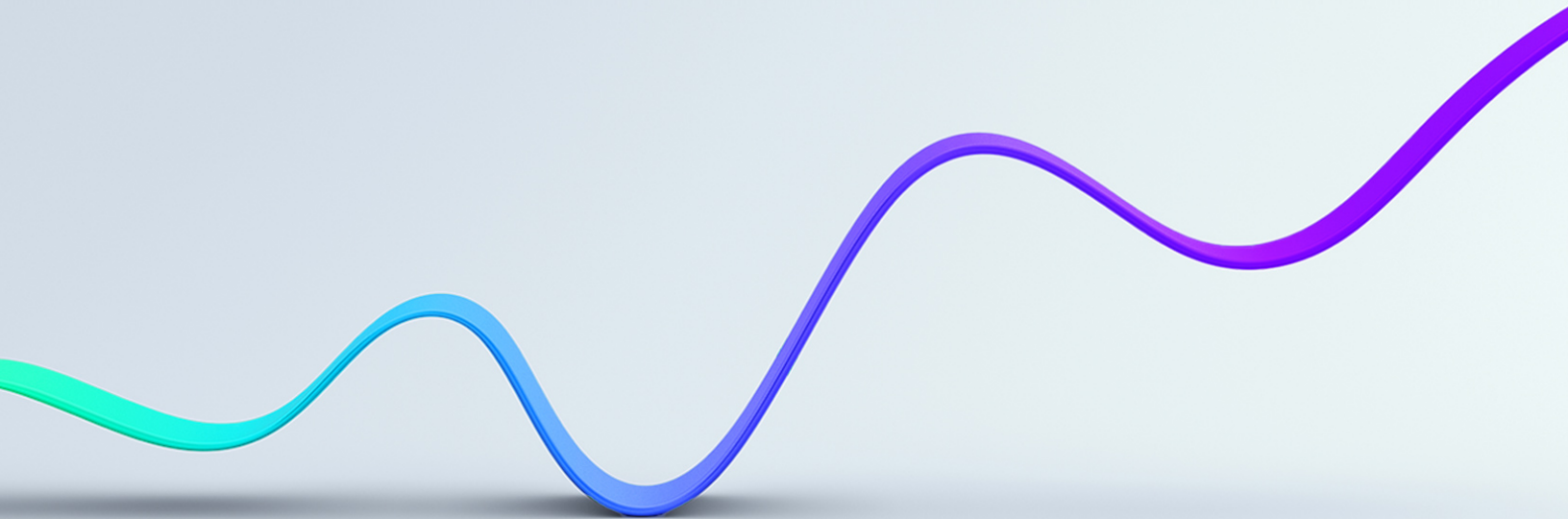


Discreet Network

# Economic Model

Revision 1.0.0

August 22, 2023



Published August 2023

Authored by Brandon Koerner & Frederik Markor

# Discreet Network Economic Model

August 22, 2023

## Contents

<b>1</b>	<b>Introduction</b>	<b>1</b>
<b>2</b>	<b>Token Distribution</b>	<b>2</b>
2.1	Pre-launch . . . . .	2
2.2	Venture capital . . . . .	2
2.3	Mainnet launch . . . . .	2
<b>3</b>	<b>Emission Schedule</b>	<b>2</b>
3.1	Tables . . . . .	2
3.2	Graphs . . . . .	3
<b>4</b>	<b>Validator requirements</b>	<b>4</b>
4.1	Financial . . . . .	4
4.2	Technical specifications . . . . .	4
<b>5</b>	<b>Conclusion</b>	<b>4</b>

## 1 Introduction

This paper serves to introduce the economic model that will power the Discreet Network. Presented here are emission schedules, tail emission projections, as well as maximum capitalization for each stage of the network, set out in consensus round intervals.

The Discreet Network utilizes a native asset called \$DIST, which is minted by validators using the network's novel consensus mechanism: Aurem. Aurem is a special type of consensus that offers instant finality, a medium committee size to avoid compromising decentralization, and a zero-knowledge circuit to keep all stakes hidden. The network utilizes \$DIST to incentivize consensus participants, and is meant to reimburse the cost of running a Discreet validator node, with an extra premium added on top as a token of goodwill for securing the network for the public.

## 2 Token Distribution

### 2.1 Pre-launch

Prior to launch, in order to allow for smooth development and community growth (as well as project growth), the following \$DIST are allotted:

- At network launch approximately 8'500'000.00 \$DIST ( 3.14% of total tokens, prior to tail emission) is distributed in a regulated pre-sale.
- Originally, 15'000'000 \$DIST were set aside for project growth, bug bounties, and future project allocation. Due to the lower initial supply prior to genesis, only 1'500'000 \$DIST will be allocated to these directly.
- The Discreet team has 5'000'000 \$DIST for community growth and grants. The team will be extending the lock on these tokens until Q3 2024.
- At network launch approximately 10'000'000 ( 3.7%) \$DIST will be sold to venture capital firms, and used for CEX (centralized exchanges) listings liquidity. These sales are subject to strict vesting schedules, and amounts that cannot meaningfully impact the market.
- The remaining amount of \$DIST prior to network genesis will be fairly distributed or burned at the discretion of the team, with full transparency to the community.
- All of the supply listed in the emission schedule below is distributed fairly amongst validators through the consensus mechanism.

Among the changes to the original token distribution prior to launch, on Aug. 16th 2023, the Discreet team decided to burn 12'126'135.5 \$DIST that were in possession of the team, allowing for the very low circulating supply that the chain will launch with. The reasoning behind this was to ensure that all \$DIST would be sufficiently distributed in a decentralized manner, as well as keep most \$DIST available as validator incentives.

### 2.2 Venture capital

Should Discreet decide to seek venture capital, the allocations will be limited per entity to keep no single actor from meaningfully impacting or manipulating the market. The project will remain as transparent about potential private seed investors as the contracts allow.

The Discreet team has good counsel on who can navigate the project in the landscape of seed allocation, and the team's vesting schedules are strict. This section only applies if the project needs to go the route of venture capital investment.

### 2.3 Mainnet launch

Once mainnet is launched, \$DIST will not be immediately listed on CEXs. This allows good opportunity for validators to familiarize themselves with the staking process prior to \$DIST becoming tradeable on CEXs.

## 3 Emission Schedule

### 3.1 Tables

The Discreet Network employs a token emission schedule to provide economic support for ensuring network security among consensus participants. Although there is a reasonable expectation that the cumulative transaction fees will progressively meet the expenditures associated with upholding the protocol's security, the initial stages of the protocol's development necessitate the issuance of tokens to complement the revenue generated from transaction fees. The specific delineation of the token emission schedule is explicated in the following table:

\$DIST Emission Schedule			
Consensus level Interval	Emission Per Block	Emitted Amount	Total supply
1 - 9'000'000	5 \$DIST	45'000'000 \$DIST	90'000'000 \$DIST
9'000'001 - 18'000'000	3 \$DIST	27'000'000 \$DIST	117'000'000 \$DIST
18'000'001 - 27'000'000	2 \$DIST	18'000'000 \$DIST	135'000'000 \$DIST
27'000'001 - 37'000'000	1.6 \$DIST	16'000'000 \$DIST	151'000'000 \$DIST
37'000'001 - 45'000'000	1.5 \$DIST	12'000'000 \$DIST	163'000'000 \$DIST
45'000'001 - 50'000'000	1.4 \$DIST	7'000'000 \$DIST	170'000'000 \$DIST
50'000'001 - 70'000'000	1.2 \$DIST	24'000'000 \$DIST	194'000'000 \$DIST
70'000'001 - 100'000'000	1.0 \$DIST	30'000'000 \$DIST	224'000'000 \$DIST
100'000'001 - 120'000'000	0.8 \$DIST	16'000'000 \$DIST	240'000'000 \$DIST
120'000'001 - 140'000'000	0.6 \$DIST	8'000'000 \$DIST	252'000'000 \$DIST
140'000'001 - 160'000'000	0.4 \$DIST	8'000'000 \$DIST	260'000'000 \$DIST
160'000'001 - 200'000'000	0.25 \$DIST	10'000'000 \$DIST	270'000'000 \$DIST
200'000'001 - $\infty$ <sup>*TE</sup>	0.15 \$DIST	-	-

*\*TE: This is the tail emission amount. This amount will be awarded to block validators in perpetuity after the last block schedule has lapsed.*

### 3.2 Graphs

The following present the information from the table in two graphs.

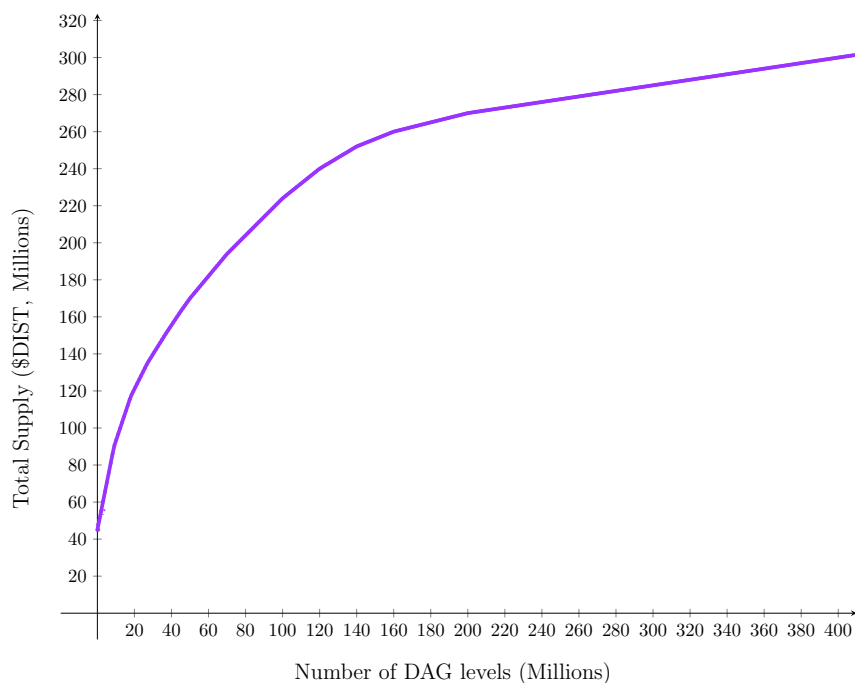


Figure 1: Total supply of \$DIST versus the number of levels added to the DAG (serves the role of blocks in a DAG). The supply begins low to allow for mined coins to add to the privacy of the network and support validators via incentives, and caps off at a fixed emission rate after sufficient height.

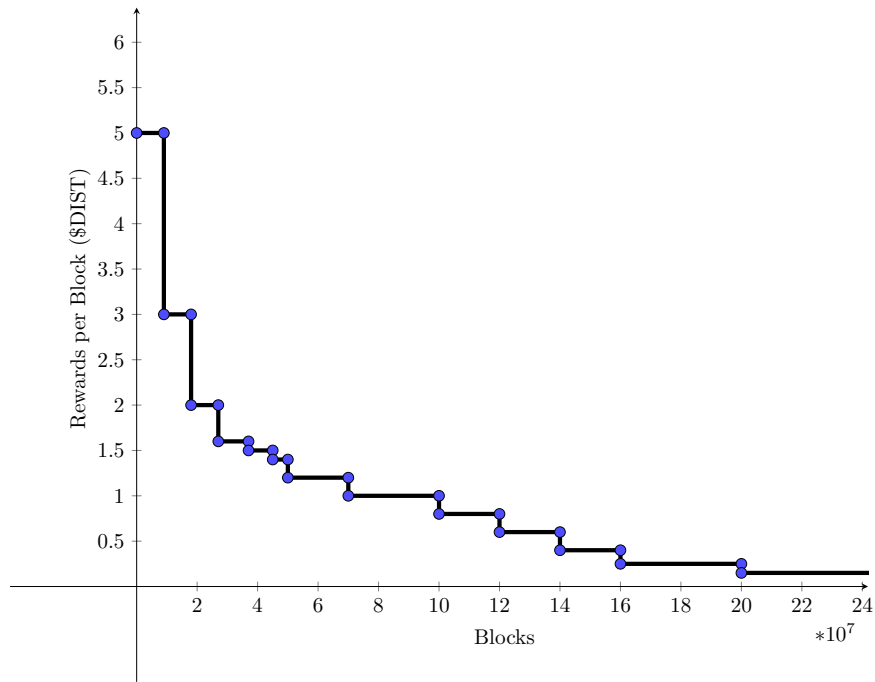


Figure 2: The block reward versus the number of consensus rounds. This shows the reward curve from genesis to when tail emissions occurs.

## 4 Validator requirements

### 4.1 Financial

To participate in the Discreet consensus committee, a validator *must commit 20'000.00 \$DIST as the minimum collateral* used for the staked amount. If a node exhibits byzantine behavior (whether malicious, unresponsive, or not kept up-to-date), the collateralized \$DIST stake will be slashed permanently (i.e, no node will receive this slashed amount and the tokens will be unrecoverable).

### 4.2 Technical specifications

Validators should have at least a 500 Mbit/s connection, in both upload and download, have 64 gigabytes of fast RAM, as well as a dedicated Internet line with consistent, reliable up-time (i.e. a data center or server). Hardware for the validators should have a modern multi-core processor capable of computing the required zk-STARK proofs in an appropriate amount of time. Additionally, validator hardware should be able to check up to the theoretical limit of transactions per second as shown in tests of Aurem. Users wanting to check their hardware can launch a validator on the Discreet testnet before staking on mainnet to ensure sufficiency to the above requirements/recommendations.

## 5 Conclusion

In the pursuit of maintaining a robustly decentralized coin supply for the \$DIST network, a strategic decision has been made to enact a token burn exceeding 90% of the initial tokens allocated for launch. This discerning approach entails reallocating these tokens to a mining pool, thereby fostering an environment of permissionless participation and decentralized acquisition. Central to this initiative is the novel Confidential Proof-of-Stake consensus mechanism, Aurem, which underscores the network's commitment to technologically advanced and equitable engagement.

The imperative to cultivate a thriving ecosystem has guided the redirection of tokens toward validators committed to network safeguarding and users seeking to possess \$DIST. This deliberate allocation realignment signifies a commitment to buttress network security while bolstering the user base, achieving a symbiotic relationship between security and accessibility.

The implementation of these profound measures to aggressively burn team-held tokens reflects the project's dedication to establishing and maintaining a balanced coin distribution, thereby mitigating the risks associated with centralization and fostering a sustainable network.

This paper has contributed to a comprehensive understanding of the essential requisites for operating a Discreet node, as well as the intricate economic model guiding the trajectory of the network. With careful consideration and meticulous research as the backdrop, prospective validators are poised to embark on the forthcoming stages of engagement. In preparation, prospective validators are required to meet the stipulated \$DIST collateralized asset criteria, facilitating their participation in the network's integrity.

As the next phase beckons, the discreet.net website will provide a page for aspiring validators to alert the team of their interest, akin to the precedent set by the alpha testnet sign-up process. This exclusive early staking alpha testing phase not only invites validators into a collaborative environment but also paves the way for refining and enhancing the \$DIST network through valuable insights and real-world experimentation.