



Midnight tokenomics and incentives whitepaper

May 2026 / Version 1.81



Abstract

This white paper describes the composite tokenomics of Midnight, centered around NIGHT, Midnight's native utility token, and DUST, the network resource used to pay for transaction fees; it outlines their key functions, utilities, and properties, including the unique token-generates-resource dynamic relationship; it describes Midnight's approach to incentives and rewards to promote block production and network security; it offers a view of Midnight's cooperative tokenomics and mechanisms for network access expansion and a multi-chain future; and it describes the initial distribution mechanism and token allocation.

Legal disclaimer

The information provided herein is for informational purposes only and should not be construed as financial, legal, or investment advice. We and our affiliates do not recommend that NIGHT or DUST or any digital assets be bought, sold, swapped, staked, or held by you. It is the responsibility of any person who accesses the information herein to observe all applicable laws and regulations of their relevant jurisdiction. By proceeding to obtain the information, you are representing and warranting that all the applicable laws and regulations of your jurisdiction allow you to access such information. We and our affiliates make no representations or warranties of any kind, express or implied, regarding the accuracy, completeness, or reliability of the information contained herein. We and our affiliates assume no liability for any losses or damages that may result from reliance on the information contained in this document. This document may contain forward-looking statements that are subject to risks and uncertainties that could cause actual results to differ materially from those expressed or implied by such statements. Forward-looking statements in this document represent our judgment as of the date of the document. We do not undertake any obligation to update or revise any forward-looking statement to reflect new information or future events. You should not place undue reliance on forward-looking statements contained in this document.

Table of contents

1. Introduction	5
2. The NIGHT token	6
Key features/properties	6
NIGHT stakeholders	6
Genesis and token states	7
Block production rewards	10
Decentralized on-chain governance	10
On-chain Treasury	11
NIGHT-generates-Dust	11
Token Utility	12
3. The DUST resource	13
Key features/properties	13
DUST mechanics	14
DUST beneficiaries	16
Transaction handling and congestion control	16
Transaction fees	17
Dynamic pricing	18
4. Cooperative tokenomics	20
Expanding network access: capacity marketplace	20
Expanding network reach: multichain	23
5. Block production and incentives	24
Block Production at Launch	24
Moving Toward Permissionless	24
Cardano SPOs and Midnight block production	24
Producing Midnight blocks	24
Block rewards and the Reserve	24
Understanding Midnight block rewards	26
Incentivizing full blocks	28
Summary: calculating block rewards	31
6. NIGHT token distribution	33
Process overview	33
Claim phase 1: Glacier Drop	34
Claim phase 2: Scavenger Mine	37
Genesis block and mainnet launch	40
Redemption period and thawing	41
Claim phase 3: Lost-and-Found	42
Timeline	44
7. Business Model	48
Core Participants and Stakeholders	48
Dual-component economy and shielded technology	49
Governance and Midnight Improvement Proposals (MIPs)	50
Cooperative tokenomics: capacity-marketplace components	51
8. Roadmap	20
The four phases of Midnight's development	20
9. Glossary	20

Table of contents

1. Introduction	5
2. The NIGHT token	6
Key features/properties	6
NIGHT stakeholders	6
Genesis and token states	7
Block production rewards	10
Decentralized on-chain governance	10
On-chain Treasury	11
NIGHT-generates-Dust	11
Token Utility	12
3. The DUST resource	13
Key features/properties	13
DUST mechanics	14
DUST beneficiaries	16
Transaction handling and congestion control	16
Transaction fees	17
Dynamic pricing	18
4. Cooperative tokenomics	20
Expanding network access: capacity marketplace	20
Expanding network reach: multichain	23
5. Block production and incentives	24
Block Production at Launch	24
Moving Toward Permissionless	24
Cardano SPOs and Midnight block production	24
Producing Midnight blocks	24
Block rewards and the Reserve	24
Understanding Midnight block rewards	26
Incentivizing full blocks	28
Summary: calculating block rewards	31
6. NIGHT token distribution	33
Process overview	33
Claim phase 1: Glacier Drop	34
Claim phase 2: Scavenger Mine	37
Genesis block and mainnet launch	40
Redemption period and thawing	41
Claim phase 3: Lost-and-Found	42
Timeline	44
7. Business Model	48
Core Participants and Stakeholders	48
8. Roadmap	49
The Four Phases of Midnight's Development	49
9. Glossary	51

1. Introduction

Early blockchain implementations, with their unrestricted access to data and metadata, evolved around radical transparency as a way to enable trustless integrity within a decentralized environment. Unwarranted side-effects to this approach include exposing sensitive data, like financial information, medical records, and trade secrets, compromising on data protection to the point of facing compliance issues. This makes most major public blockchains unsuitable for many real world use cases.

Traditional tokenomic models rely on a single token and require users to spend tokens for every transaction, creating economic uncertainty due to token price volatility. Further, their Initial token distributions often favor insiders and early investors, concentrating control among a small group while failing to provide the opportunity for broad, meaningful community participation. On a larger scale, these same blockchains take a closed-loop, inward-looking approach to their economies, in which value is siloed and mostly bounded by the confines of a single network. This adversarial approach focuses too much on competition, and too little on cooperation. This winner-take-all mentality has led to a highly fragmented ecosystem that fails to unlock the immense value that lies in cross-chain collaboration.

The Midnight protocol introduces a novel approach to blockchain tokenomics designed to overcome these challenges. This approach achieves privacy, scalability, and interoperability through a distinctive dual-component tokenomics system designed to foster predictable operations, broad participation, and cross-chain value creation. Broadly, the core pillars underpinning Midnight's tokenomics are:

- **Operational predictability:** Midnight's native token, NIGHT, continually generates DUST, the renewable resource used to pay for transactions. NIGHT holders can execute transactions for as long as they hold enough tokens to generate the amount of DUST required. This design provides predictable operating costs that are not directly linked to the price of the native token.
- **Rational privacy:** DUST is a shielded resource, meaning Midnight transactions – like interacting with a DApp – do not leave a trail of metadata in the same way a single-token architecture would. Unlike privacy coins, the DUST resource is designed with compliance with laws and regulations in mind.
- **Cooperative tokenomics:** Midnight's multichain architecture expands access and extends its utility beyond the network and across the Web3 space, fostering cooperation and cross-chain value creation. Users can pay for transactions with other blockchains' native tokens, or even with fiat currencies. Much like traditional Web2 models, DApp operators can sponsor their users' operations.
- **Fair by design:** through a free, multi-phase, transparent, and fair token distribution beginning with the Glacier Drop, Midnight aims to bootstrap a diverse community of engaged participants.

While the technical architecture sits outside of the scope of this whitepaper, the components and mechanisms that make up Midnight's tokenomics and incentives system are described below.

2. The NIGHT token

NIGHT is Midnight's utility token whose main function is to generate DUST, the resource used to execute transactions on the Midnight network. It is intended that NIGHT will also be used for block production rewards, ecosystem growth incentives, and on-chain governance in relation to the Midnight network. One unit of NIGHT is further divided into one million subunits called STARS. The key features of NIGHT are expected to be as follows:

Key features/properties

- **Unshielded:** the NIGHT token is unshielded, meaning NIGHT transactions are stored and publicly visible on the blockchain – including metadata, such as wallet addresses, values, and timestamps.
- **Transferable:** NIGHT can be freely transferred between wallets, listed on exchanges, and independently wrapped, bridged, and represented across various networks, including Cardano and Midnight. NIGHT was not listed on exchanges as part of the initial token distribution, but has subsequently been listed on various exchanges (including EU crypto-asset trading platforms).
- **Token supply:** 24 billion NIGHT tokens minted on Cardano, which are mirrored on the Midnight network.
- **Non-expendable:** NIGHT is not expendable to execute transactions.
- **Disinflationary:** the expansion of the circulating supply via block rewards slows down over time, until the full supply is circulating and no more inflation occurs.
- **Broad distribution:** the broad, open, and inclusive nature of the NIGHT token initial distribution (as described in the corresponding section) ensures that the benefits of the network are widely shared across the Web3 space and beyond.
- **Multi-chain:** in contrast with wrapped token representations, NIGHT exists natively and maintains the same properties and rights both on Cardano, as a Cardano Native Asset, and on Midnight, as the blockchain's native token.

NIGHT stakeholders

The core network constituents and NIGHT token stakeholders in the Midnight economy are:

- **NIGHT token holders:** the collective of users who make use of the NIGHT token and who are expected to control future network and ecosystem development via a decentralized governance mechanism.
- **Midnight block producers (MBPs):** network participants who elect to run Midnight validating nodes, block producers receive rewards for validating Midnight blocks and securing the network.

- **Midnight Foundation:** a foundation whose mission is to promote long-term ecosystem development and stewardship.
- **Midnight TGE:** a subsidiary of the Midnight Foundation, whose primary role is to run and manage the NIGHT token supply creation, issuance, and distribution.
- **On-chain Treasury:** a pool of funds earmarked for ecosystem growth activities, initially locked by the protocol and expected to be managed by the community via a future decentralized governance framework.
- **Reserve:** a special constituent of the Midnight economy, the Reserve is a protocol-managed pool of tokens whose function is to issue block production rewards to Midnight block producers.

Genesis and token states

The NIGHT token has a supply of 24 billion tokens. The total NIGHT supply will be minted on the Cardano blockchain at the beginning of the token distribution, after which tokens can exist in either one of two states: *uncirculated* or *circulating*.

- **Uncirculated** tokens consist of NIGHT tokens earmarked for block production rewards held by the Reserve.
- **Circulating** tokens consist of all other tokens, including those belonging to the community and other core network constituents.

NIGHT tokens may enter into circulation in two ways: as part of the token distribution process or as block production rewards. All issuance of tokens into circulation outside the token distribution phases happens in the form of block production rewards coming from the pool of *uncirculated* tokens allocated to the Reserve.

Multi-chain token

When the Midnight mainnet launches, the genesis block will contain a mirror image of the NIGHT tokens on Cardano. As a result, NIGHT will exist natively on Cardano (as a Cardano Native Asset) and on the Midnight mainnet (as the network's native token).

Circulating NIGHT tokens will manifest in one of two states: *protocol-locked* and *protocol-unlocked*:

- **Protocol-locked** tokens cannot be moved or perform any functions, such as generating DUST resources or being used for governance actions.
- **Protocol-unlocked** tokens can be moved by their owners and carry full utility.

Every *protocol-unlocked* token on Cardano will initially be *protocol-locked* on Midnight, and vice-versa. This ensures an initial state where no token will be unlocked on both chains at once. A cross-chain software protocol will then ensure that whenever tokens are issued/put in circulation on Midnight, a corresponding amount of tokens will be automatically locked on Cardano, such that this constraint is never violated on an ongoing basis.

This is designed to ensure that the effective total supply of NIGHT does not exceed 24 billion. This cross-chain mechanism will be enforced at the protocol level and only applies to NIGHT tokens that are natively issued on Cardano and Midnight.

There is a planned protocol-level bridge that will enable one-way transfers of NIGHT tokens natively from Cardano to Midnight. These tokens will enter circulation in the *protocol-unlocked* state on the Midnight network (thus becoming *protocol-locked* on Cardano, as per the cross-chain software protocol). However, there will not be, by mainnet launch, a protocol-level bridging mechanism to natively facilitate transfers in the opposite direction, from Midnight to Cardano. It is expected that a two-way bridging mechanism will be developed after mainnet launch. However, any third party can potentially build independent bridges or their own cross-chain applications to represent NIGHT tokens across any network they choose. NIGHT tokens that may be wrapped, bridged, or otherwise represented in these (or other) networks by third parties do not carry the rights or utility of the underlying tokens they represent. Such third party solutions have no negative effect on the integrity of the cross-chain software protocol.

When expected developments in the network enable the conditions that allow the distribution of block rewards to begin, *uncirculated* tokens from the Reserve will enter circulation in both networks, in a *protocol-locked* state on Cardano and a *protocol-unlocked* state on Midnight. This pool is finite; once the Reserve is exhausted, the circulating supply will match the total supply in accordance with the rules encoded and enforced by the protocol itself.

Cross-chain token invariants

The total supply of NIGHT is balanced across the Cardano and Midnight networks. It must not be possible for the “same” token to be held by any wallet on both chains at the same time. In reality, this is not meaningful because NIGHT tokens are fungible and have different representations on each of the two chains. However, as a metaphor, it captures the key scarcity requirement for Midnight, related to the preservation of tokens in a ledger.

Another approximation of the cross-chain invariants is based on the total number of tokens in each of the three states on both chains. Let $S = 24 \text{ billion}$ be the total supply of NIGHT. The three states are: in *reserve* (R), *locked* (L), and *unlocked* (U). The chains are Cardano (C) and Midnight (M), making up for six combinations of token states and locations, hereby designated $C.R$, $C.L$, $C.U$, $M.R$, $M.L$, and $M.U$.

Since every token is represented on both chains, it is possible to begin with the firm invariant that:

$$C.R + C.L + C.U = M.R + M.L + M.U = S$$

The idealized invariants as tokens move between states are given by the following equations:

1. $C.R = M.R$ (both chains faithfully track the uncirculated reserve)
2. $C.L = M.U$ (all tokens unlocked on Midnight are locked on Cardano)
3. $C.U = M.L$ (all tokens unlocked on Cardano are locked on Midnight)

The idealized invariants are not possible in practice because it takes time for a change on one chain to be reflected on the other. Instead, they are replaced with invariants that account for this propagation delay.

The direction of the invariants is chosen to always err on the side of having fewer tokens unlocked than would be unlocked in the idealized system, preventing double-spend exploits across the chain. The actual invariants are:

1. $C.R \leq M.R$

If Cardano has released block rewards from C.R, Midnight will eventually observe that fact and release corresponding tokens as well; Midnight will not release reward tokens it has not seen released on Cardano.

2. $M.U \leq C.L$

If a token is unlocked on Midnight, it must first be locked on Cardano.

3. $C.U \leq M.L + (M.R - C.R)$

The number of unlocked tokens C.U on Cardano may exceed the number of locked tokens M.L on Midnight, but the difference between those totals must be bounded by the number of reserve tokens M.R on Midnight minus the number of reserve tokens C.R on Cardano.

Together, these invariants enforce the following inequality, akin to a version of “the same token cannot be held by any wallet on both chains at the same time”:

$$M.U + C.U \leq S$$

These invariants hold even when Cardano cannot observe Midnight. This allows Midnight to roll out cross-chain observability in stages without violating these key invariants.

In the first stage, as part of a planned protocol-layer, one-way bridge, Midnight will be able to observe the movement of tokens from C.U to C.L. When that occurs, Midnight will be able to follow this and move the corresponding number of tokens from M.L to M.U.

When network conditions and development allow for block rewards distribution to begin, uncirculated Reserve tokens will periodically move from C.R to C.L as Cardano releases block rewards. Observing this, Midnight would then move the corresponding number of tokens from M.R to M.U.

Later, when Cardano is able to observe state changes on Midnight, a two-way protocol-layer bridge will be established, allowing Cardano to also track movement of tokens from M.U to M.L. Cardano will then be able to observe this and move corresponding tokens from C.L to C.U.

The token invariants are maintained through all these possible roll-out stages, ensuring the integrity of the token supply.

At a later stage, ownership of the Reserve tokens may move from C.R to M.R, allowing Midnight to control the release of reward tokens. This change has a significant but symmetrical impact on the invariants. Once the supply has moved, it is Cardano that might lag Midnight in its understanding of the circulating tokens. As soon as that transfer of control is effected, the new invariants are:

1. $M.R \leq C.R$

2. $C.U \leq M.L$

3. $M.U \leq C.L + (C.R - M.R)$

These revised invariants reflect the delay in Cardano’s ability to reflect Midnight’s release of tokens from M.R. Just as before, they ensure the integrity of the token supply.

Block productions rewards

Sometime after the Midnight mainnet launch, the distribution of NIGHT tokens from the Reserve as rewards to Midnight block producers will start. This distribution will follow the network's block production reward distribution logic (described in the corresponding section further down this document). Once the Reserve of uncirculated NIGHT tokens is exhausted, the circulating supply will match the total supply, and rules encoded and enforced by the protocol itself guarantee that no new tokens will be created or come into circulation.

Decentralized on-chain governance

Following the launch of the Midnight network, a phased approach is expected to be implemented to progressively decentralize the Midnight governance framework, expanding on-chain governance participation.

This approach aims to enable the creation and establishment of a comprehensive set of community-centric governance tools and processes, including the drafting and submission of proposals, Treasury access to fund such proposals, voting mechanisms, vote tallying, outcome communication, and automated protocol updates for proposals approved through governance action.

The governance framework will be designed to uphold high standards of security, and to ensure the integrity of the Midnight network while enabling remediation capabilities through decentralized means. The full specification and mechanics of such governance are expected to be detailed in a future document.

Governance at launch

At launch, and during the current federated phase of operation, modifications to the Midnight protocol and to the Midnight-related parameters operating on the Cardano network are made by a governance committee operating under a multisig mechanism with a defined approval threshold. The committee currently comprises two bodies: the Technical Authority (the "TA"), a 9-member technical governance body responsible for independently evaluating and approving governance actions on technical grounds; and the Council, a 6-member governance-legitimacy body responsible for independently approving governance actions on behalf of the ecosystem. On-chain actions require approval by at least 6 of the 9 TA members and at least 4 of the 6 Council members. The committee's scope of authority includes (i) updating Midnight-related parameters on the Cardano network (including the composition of the governance committee itself and the set of federated block producers); and (ii) updating the Midnight protocol — including version upgrades, hard forks and the protocol's core parameters (such as block size and ledger parameters).

This committee is expected to be composed of various entities that have yet to be identified or formed, and is expected to be responsible for, among other things, the following:

- Updating Midnight-related parameters on the Cardano network (e.g., governance committee members, federated block producers).
- Updating the Midnight protocol (version upgrades and hard forks) and the protocol's core parameters (e.g., block size, ledger parameters).

As the Midnight network matures and its governance framework evolves, it is intended that all components of the system, including critical elements such as monetary policy, may become subject to change through on-chain governance, provided a predefined voting threshold is met. This ensures that the network retains flexibility to adapt to future needs and stakeholder consensus.

On-chain Treasury

The on-chain Treasury is a pool of NIGHT tokens belonging to the protocol and initially locked, whose purpose will be to fund Midnight network ecosystem growth activities and projects that are selected via the on-chain governance mechanics. NIGHT tokens allotted to the Treasury will be stored in the ledger, owned by the protocol, and initially locked, with a view to being unlocked when the expected on-chain decentralized governance mechanism for the Midnight network is implemented.

Neither the use of NIGHT for governance purposes nor the use of NIGHT from the on-chain Treasury to promote ecosystem growth initiatives will be available at mainnet launch. These functionalities are expected to be developed and implemented in the future.

NIGHT-generates-DUST

Midnight's dual-component tokenomics segregates block production rewards from transaction handling fees, and splits these functions between the NIGHT token and the DUST resource.

NIGHT tokens generate DUST, the shielded network resource whose only use is to pay for transaction fees that power operations on the Midnight network – that is, to enable the execution of transactions while managing network congestion and mitigating the risk of denial-of-service attacks. NIGHT will generate DUST indefinitely, meaning DUST is akin to a renewable resource (in contrast with the traditional subtractive approach that requires tokens to be expended when making a transaction).

In order to start generating DUST, a NIGHT holder must explicitly designate a DUST recipient address. DUST can only be generated in addresses on the Midnight network. The amount of NIGHT tokens held directly determines the rate at which DUST is generated into a DUST address.

At any given point in time, a variable minimum amount of DUST – dynamically adjusted according to current network demand – will be required to execute transactions via the Midnight network. While DUST will be consumed upon use, no NIGHT tokens will be expended to execute Midnight transactions.

Conceptually, this means that whoever holds NIGHT can effectively execute transactions on Midnight for free for as long as they hold enough NIGHT tokens to generate the minimum required DUST. The more NIGHT someone holds, the more DUST they generate for each period of time. This means that the higher the NIGHT holding, the higher the density of transactions – i.e., the number of transactions per unit of time – the holder has.

Token Utility

NIGHT is the native utility token of the Midnight network. Its utility under the framework set out in this tokenomics paper rests on the following functions:

- **DUST generation.** NIGHT is the resource-generating asset of the network. A NIGHT balance, once its holder designates a DUST recipient address on the Midnight network, will continually generate DUST — the shielded, non-transferable, decaying resource consumed to pay for transaction fees on Midnight — at a rate proportional to the size of the underlying NIGHT balance and up to a proportional cap, in accordance with the NIGHT-generates-DUST mechanics described in this tokenomics paper.
- **Governance (post-decentralization).** It is intended that NIGHT will function as the governance token of the Midnight network once decentralized on-chain governance has been developed and implemented. Under that future framework, NIGHT holders are expected to be able to submit and vote on proposals (including proposals affecting protocol parameters and access to the on-chain Treasury) in accordance with the governance mechanics, voting thresholds and other rules to be established for the Midnight network. The development and implementation of decentralized on-chain governance is a forward-looking matter and remains subject to the qualifications and the legal disclaimer set out at the front of this tokenomics paper.
- **MEV-resistance:** For the avoidance of doubt, the description of "utility" above is used in its ordinary commercial sense and is distinct from the regulatory classification of NIGHT under Regulation (EU) 2023/1114 ("MiCA"). As recorded in the MiCA white paper for NIGHT (at fields D.6 and G.6), NIGHT does not meet the definition of a "utility token" under MiCA: although NIGHT is intended to provide access to the functionality of the Midnight network and to have utility within it, this does not entail access to goods or services provided by Midnight TGE Ltd. as issuer (which does not control, operate or manage the Midnight network), and the provision of such access is not the sole intended purpose of the token (since, as described in item 2 above, NIGHT is also expected to be used in the decentralized on-chain governance mechanics to be developed for the Midnight network). NIGHT is accordingly classified for MiCA purposes as an "other crypto-asset" (i.e., a crypto-asset other than an asset-referenced token or e-money token), and references in this tokenomics paper to NIGHT as a "utility token" should be read accordingly.

3. The DUST resource

DUST is the shielded and renewable resource used to access *network capacity*: its single function is to enable users to execute transactions on Midnight. DUST decays over time, so it has value but cannot retain value.

DUST is analogous to electrical energy powering the Midnight network. DUST addresses serve as energy storage units, similar to battery packs. NIGHT tokens function like renewable-energy power plants, such as wind turbines, that charge battery packs up to a maximum energy storage capacity that is proportional to the size of the generating NIGHT token balance.

A NIGHT-turbine can connect to any battery pack, regardless of ownership, effectively designating its generated electricity to that storage. However, DUST-electricity is non-transferrable: once stored in a battery pack, it cannot be transferred to another battery pack; it can only be used to execute Midnight transactions. When disconnected from its generating turbine, the stored electricity has a finite shelf life, decaying linearly at the same rate it was generated.

A paper detailing the design of DUST and transaction handling dynamics is expected to be published separately.

Key features/properties

- **Shielded:** DUST allows for transactions to take place without exposing users' metadata. Wallet addresses and transaction details (like values and timestamps) are not disclosed to counterparties or made available on the public ledger.
- **Consumable:** DUST is consumed when used – meaning it is burned and does not cycle back into circulation.
- **MEV-resistance:** DUST shielding and burn reduce MEV likelihood since attackers cannot identify potential victims.
- **Renewable:** DUST is continually generated by NIGHT balances in perpetuity. This property encourages more active participation and interaction with the network, potentially leading to a more vibrant ecosystem.
- **Decaying:** a DUST balance decays when disassociated from the NIGHT address that generates it, meaning it cannot act as a store of value. For example, when a NIGHT token is transferred, the balance of DUST in the original holder's DUST wallet will decrease to 0. The recipient of the transferred NIGHT token will have to issue a new gesture to resume DUST generation at a new address.
- **Unlimited:** as it is generated continually and indefinitely, there is no limit to how much DUST can be generated over time. However, the available supply at any given point in time is capped by the number of NIGHT tokens generating DUST.

- **Non-transferable:** DUST cannot be transferred between addresses, meaning it can neither be bought nor sold – insulating it from supply shocks and volatility. This property also strengthens its utility solely as a resource to power transactions, while also addressing regulatory aspects that are commonplace with shielded assets that can act as stores of value.
- **Non-pegged:** there is no fixed 1:1 parity between the DUST and NIGHT supplies; the supply of the resource that is available at a given moment fluctuates with usage and network dynamics.

DUST mechanics

DUST is a *network resource* – meaning it is used to conduct transactions and operate in the network. On the surface, DUST is similar to a token or other fungible crypto-assets in that it is also represented by balances held at specific blockchain addresses. However, unlike traditional tokens, DUST does not exist independently of NIGHT; it does not have *permanence*. Its existence is determined and sustained by its continuous association with the NIGHT token. This association happens between NIGHT and DUST addresses in a process called designation, by which a NIGHT token holder appoints a DUST address as the recipient for resource generation.

DUST addresses are shielded, and DUST expenditures are recorded on the public blockchain using cryptographic techniques that make them visible only to the DUST owner. DUST addresses and balances are only known to the holders of the associated NIGHT token addresses who designate them.

Designation and generation

DUST comes into being when a NIGHT token holder designates a DUST address as the recipient, thus initializing the DUST generation at that address. The designated address is DUST-specific, separate, and non-derivable from the originating NIGHT address.

From that moment onwards, for as long as the associated NIGHT balance remains unchanged, the DUST balance in that address will increase over time – linearly, with each passing block – until it reaches its *DUST cap* (or until the association is severed).

A NIGHT holder can designate any DUST address as the destination for their DUST generation. This means that the DUST recipient address may or may not be controlled by the associated NIGHT balance holder (who can also *redesignate* addresses as often as they wish). This flexibility enables different categories of DUST beneficiaries, allowing for new, interesting use cases and functionalities.

DUST cap

The *DUST cap*, or the maximum amount of DUST resources that can be stored in a DUST address, is proportional to – and limited by – the balance of the associated NIGHT token address(es). As long as this balance remains unchanged, that NIGHT address will continually generate DUST to a designated DUST address – up until either its DUST cap is reached, or the association between the DUST address and the generating NIGHT is severed by the NIGHT holder. When the DUST cap is reached, DUST generation halts until some of the DUST is used.

Using DUST

In contrast with other blockchains, transaction fees on Midnight are not collected by block producers or anyone else. There is no DUST tipping mechanism to compensate block producers during transactions – nor would it make sense to have one, as the resource is not transferrable and cannot act as a store of value. When DUST is used during a transaction, it is expended and burned. If, after a transaction, the DUST balance at a given address falls below the cap, and that address remains designated as a recipient by a NIGHT address, the generation then resumes until the balance again reaches the cap (or until the association is severed).

Changes to the associated NIGHT balance

If the balance of the associated NIGHT address *increases*, or if additional NIGHT addresses designate their generation to a single DUST recipient (increasing the aggregate associated balance), the cap for that address increases proportionally, and new resources are generated until the balance hits the new cap.

If, conversely, the balance *decreases* (such as when a NIGHT holder sends some or all of their NIGHT tokens to another address), the DUST balance in the designated address decays until it reaches the new cap. If no NIGHT tokens are left, the DUST at that address will decay to zero.

Severing the association

Once a DUST address is designated, the generation process happens until the NIGHT token holder explicitly severs the association between the addresses. They can do so by:

- Transferring the associated NIGHT tokens to another NIGHT address
- Redesignating the DUST production to another DUST address
- Undesignating the production of DUST

Once severed, the DUST generation to the disassociated address stops, and the resources therein start to decay.

Dust decay and prevention of double-spending

When the association between a DUST address and the NIGHT address that generates it is severed (e.g., if the NIGHT holder either transfers or explicitly redesignates/undesignates their tokens), the DUST balance therein decays over time – with each passing block – until it disappears.

This decay happens linearly. For a given amount of NIGHT, the *aggregate* amount of associated DUST in existence can never go above the cap – as for every unit that gets generated, another unit decays. Ultimately, this mechanism prevents the double-spending of resources: even if a NIGHT holder redesignates their generation to other DUST addresses in an attempt to try and accumulate resources, the cap is still enforced.

DUST beneficiaries

- Three broad categories of users can benefit from the utility of DUST: *NIGHT* holders, *DUST* recipients, and *DUST* sponsees. Each of them is able to transact, both directly or indirectly, as described below.
- **NIGHT holders:** generate *DUST* by designating a *DUST* address of their choice. This address then functions as a resource faucet, continuously generating *DUST* for the use of its owner for as long as it remains the designated address. *NIGHT* holders can be the recipient of their generated *DUST* and can thus transact on Midnight when choosing to do so. From a user perspective:
 - *I hold NIGHT, and my NIGHT generates DUST to an address I control.*
 - *I hold NIGHT, and my NIGHT generates DUST to an address I do not control.*
- **DUST recipients:** receive *DUST* from someone else (a *NIGHT* holder), and can actively use it to execute transactions without ever having to own tokens themselves. For example, a non-profit application that requires *DUST* to operate can rely on designations to run their operations without having to acquire *NIGHT*. From a user perspective:
 - *I hold DUST in an address I control, but I do not hold the associated NIGHT or any NIGHT.*
 - *I hold DUST in an address I control, but I hold unassociated NIGHT.*
- **DUST sponsees:** do not receive *DUST*; instead, their transactions are “covered” by a *DUST* recipient (who themselves may or may not hold *NIGHT*) when they execute a transaction. Usually, this will happen when a user interacts with the interface of an application that runs on Midnight. For example, a decentralized e-commerce application can sponsor the usage of their application, covering the *DUST* cost of every customer who makes a purchase without the users ever being exposed to the complexities of Web3. *DUST* sponsees are not required to hold *NIGHT* or have direct access to *DUST*. In fact, they do not even need to know that there is a blockchain, as the application can handle the entire process on their behalf. From a user perspective:
 - *I hold neither DUST nor NIGHT, and my transactions are paid for by a DUST holder.*

Transaction handling and congestion control

Midnight’s transaction handling approach aims to strike a balance between mitigating network congestion – both organic and malicious – and ensuring that transaction costs can maintain a relative degree of stability. To achieve that, Midnight applies a dynamic pricing model that automatically – and continually – adjusts the cost of transactions to account for network demand and computational resources utilization.

¹ Midnight transactions are denominated in the *DUST* resource; the use of terms like fee, cost, or price does not imply real-world monetary value. As already established, *DUST* cannot hold value or be transferred between addresses.

Transaction fees

Midnight transaction fees are made up of three components that are used to calculate the DUST cost of each individual transaction:

- **A minimum fee**, a small fixed fee payable in every transaction;
- **A congestion rate**, a dynamic multiplier based on network demand;
- **A transaction weight**, based on computational resources required.

Minimum fee

The *minimum fee* is a configurable system parameter that is payable in every transaction, irrespective of network usage, transaction size, or complexity. It ensures every transaction has a minimum cost. Its primary function is to prevent denial-of-service (DDoS) attacks by making it prohibitively expensive – in DUST terms – for an attacker to indefinitely sustain millions of small transactions that might disrupt the network over extended periods.

Congestion rate

The *congestion rate* is the dynamic component of the transaction fee that is adjusted at each block to account for network demand and utilization. It is a variable multiplier, measured in DUST-per-byte, that applies to each operation's *transaction weight* (see next subsection). The goal of the congestion rate is to ensure that the cost of transactions can rise or fall to match network conditions. Lower transaction costs during quiet periods should stimulate more activity, whereas higher fees during high-traffic periods should discourage transactions. Congestion rate is based on the following factors:

- The *fee adjustment factor*, a function of the current block's utilization rate in relation to the block utilization target;
- The *congestion rate* for the previous block/epoch.

The congestion rate at block n can be summarized as:

$$CongestionRate_n = CongestionRate_{n-1} * (1 + FeeAdjustmentFactor)$$

By taking into account not just the current block utilization, but also that of the previous block, this model can react to trends in network usage.

Transaction weight

Initially, the *transaction weight* will reflect the amount of storage space required by an individual transaction, measured in kilobytes (KB). Given that a Midnight block is limited in size (by a system parameter), there are only so many transactions that can fit within a single block. Transaction weight is expected to be expanded to include other relevant factors for network activity, such as compute and disk read usage.

Transaction fee summary

The transaction fee composition for a given transaction at block n can be fundamentally described as:

$$TxFee_n = CongestionRate_n * TxWeight + MinFee$$

Block utilization target

Midnight targets a block utilization rate of 50%. This value is a system parameter that can be adjusted via governance action. The goal of this target is to balance critical factors like network security, decentralization, and the economic principles surrounding scarcity of block space.

There are no inherent technical restrictions preventing a blockchain from increasing the size of its blocks. Block space is an abstract concept within blockchain technology, and block size limits are calculated design choices. However, such changes can have profound implications to the network. From a security and decentralization standpoint, smaller blocks are generally preferred. Larger blocks require more processing power and storage capacity, which can lead to centralization – as only a few powerful participants might be able to afford the computational resources to operate full nodes. This can undermine network security, as decentralization is key to the robustness and integrity of blockchain systems.

Economically, block space is a scarce resource bound by both size and time interval. Fundamentally, the available block space per time window is what bounds Midnight's transaction throughput. Imposing a size limit, or targeting a specific level of block fullness, such as 50%, instead of maximizing it to 100%, strategically controls this scarcity. Operating at full capacity leaves no room for fluctuations in demand, potentially leading to consistently high transaction fees and delayed transaction processing during peak times. Conversely, setting too low a target disincentivizes transactions and all network activity.

Optimally, setting a target at 50% fullness ensures there is always spare capacity available to accommodate sudden increases in transaction volume without significant delays or fee increases.

Dynamic pricing

The mechanism by which this operates can be described as *dynamic pricing*. When demand for block space increases and blocks begin filling beyond the 50% target, transaction fees start to rise. This increment in fees continues until the cost becomes prohibitive for some users – who then opt out, causing a reduction in demand.

Congestion and transaction spam

Dynamic pricing comes into play not just to regulate costs in times of peak demand, but also when it comes to disincentivizing sustained transaction congestion – malicious or not – in which rational or irrational participants flood the network with valueless transactions.

Most blockchains have built-in incentives against transaction spamming because each transaction incurs a *monetary cost* that depletes a scarce resource.

Midnight's NIGHT-generates-DUST mechanism does not prevent attackers from spamming the network with useless transactions for as long as their NIGHT holdings allow; similarly, block producers might be incentivized to fill blocks with valueless transactions to capture the variable share of block rewards. Both scenarios resemble a smaller version of a demand spike.

However, the increased DUST cost coupled with the intrinsic computational costs of generating ZK proofs have the effect of disincentivizing transaction spamming. Whenever a shielded resource like DUST is consumed by use, a ZK proof is needed to justify the existence of ownership of the DUST amount being spent – which incur computational costs. If transaction fees rise due to high demand, transactions without enough DUST are rejected for insufficient DUST, requiring resubmission – which includes a new ZK proof to support the new DUST spend. Generating a ZK proof is much more costly than verifying it, creating an asymmetric, self-inflicted cost for potential attackers. This design discourages rational actors, and irrational actors will eventually deplete their DUST holdings, preventing sustained attacks.

A self-regulating stabilizer

If, conversely, blocks consistently run below 50%, transaction fees will decrease, making it economically viable for more users to execute transactions. This elasticity in transaction costs serves as an automatic stabilizer for the network, adjusting to the demand and supply of block space, and ensuring that blocks are neither too empty (which would suggest underutilized network capacity and unnecessarily low transaction fees) nor too full (which could lead to slow transaction times and high fees).

This self-regulating system helps maintain the block fullness near the targeted 50% under typical conditions. This equilibrium mechanism not only optimizes network efficiency, but also stabilizes transaction costs over time – which is essential for both regular users and businesses relying on the network. Thus, the 50% block fullness target isn't just a technical parameter; it's a crucial economic setting that ensures the blockchain remains secure, decentralized, and functionally efficient.

4. Cooperative tokenomics

Despite their permissionless nature, the tokenomics of most major public blockchains motivate network participants to remain within the boundaries of a single ecosystem, accessible via a single token, reducing the economic incentives to work with – and across – other networks.

Midnight aims to break free from this paradigm to create a truly interoperable layer with cross-chain incentives, becoming the **connecting tissue across all kinds of networks**, be these blockchains or not. This section explores some emerging functionalities, enabled by Midnight's cooperative tokenomics and multichain architecture, that support this vision of an **interconnected** and **interoperable** future for Web3.

Expanding network access: capacity marketplace

Capacity marketplace is a concept that describes the different potential solution designs that can offer non-Midnight users frictionless access to Midnight network capacity while also benefiting the Midnight economy. In essence, the development of a capacity marketplace would benefit:

- **Non-Midnight end-users:** could tap into Midnight apps and functionality without having to hold NIGHT or understand DUST mechanics – or to even know they exist. Any token – and even fiat – could potentially be used to access Midnight transactions.
- **DApp operators:** can sponsor transactions for their users using any token (or even fiat currencies) if they don't have access to sufficient DUST.
- **NIGHT holders:** could get a potential revenue stream by leasing or selling their unused DUST.
- **Midnight Treasury:** could unlock a new source of funding, be expanded to hold assets other than NIGHT on Midnight, and even diversify and hold assets in other networks.

Defining network capacity

It is useful to define what is meant by *network capacity*. For the purposes of this exploration, capacity represents the amount of on-chain work that can be performed by the network. Midnight network capacity is bounded in time by how much work can be performed at each block. Capacity is measured – and dynamically priced – in units of DUST resource. A Midnight DApp user utilizes DUST to secure network capacity and execute transactions.

Accessing network capacity

From an end-user perspective, Midnight capacity can be accessed *directly* (by owning and using DUST to execute transactions) or *indirectly* (by having one's transactions be sponsored by a DUST holder).

- **Direct access:** DUST can be accessed and used directly by users who either own NIGHT tokens – and thus designate their own DUST address to receive the generated resources – or who are the recipients of DUST generated by NIGHT tokens owned by someone else.
- **Indirect access:** Although access to network capacity requires DUST, from an end-user perspective, access to Midnight can be abstracted by application developers. DUST resources required to execute transactions can be paid by – or on behalf of – the end-user, granting them access to Midnight DApps without requiring them to own, use, or even be aware of the underlying blockchain. This allows for effectively tokenless, blockchain-abstracting applications.

Capacity marketplace paradigms

A marketplace's function is to match buyers and sellers while allowing for optimal price discovery. With blockchain technology, marketplaces exist on a spectrum ranging from mostly off-chain, centralized applications, to decentralized solutions enabled by protocol-level primitives.

Midnight's capacity marketplace is expected to offer different solutions that compete on efficiency, price, and specialization. Below are some examples of potential offerings.

Off-chain marketplace models

The simplest form of matching is a peer-to-peer exchange, where a NIGHT holder designates their DUST generation to an address controlled by another user in exchange for a payment settled off-chain, either directly or facilitated via a broker. For that reason, off-chain marketplaces are more centralized and require a level of trust between parties. However, when trust exists, they can also be highly efficient and flexible – for example, enabling fiat payments. Examples of this paradigm include:

- **DUST generation leasing:** NIGHT holders lease their DUST by designating the DUST generation directly to a lessee's DUST wallet. The lessee can then use DUST however they want, for as long as they maintain the lease. Arrangements between parties, as well as any payments, are settled off-chain.
- **Broker-managed leasing:** NIGHT holders lease their DUST via specialized brokers, who then coordinate the DUST generation lease from one or more lessors to one or more DUST lessees. Brokers then facilitate payments to lessors, collecting a fee for their services. This model has the advantage of being scalable, thus enabling competition and potentially more efficiency.
- **Babel Station:** a service that allows users to create and submit transactions without including DUST by means of Midnight's implementation of ZSwap²– a transaction scheme that provides a provably secure and data-protecting mechanism for atomic asset swaps. Users submit their transactions with a ZSwap intent – an offer or statement of a desired future – including non-NIGHT tokens (or fiat) as payment.

² <https://docs.midnight.network/learn/understanding-midnights-technology/zswap>

If accepted, the station operator submits the transaction containing the necessary DUST on behalf of the user. The Babel Station acts as a “DUST filling station”, giving anyone on-demand indirect access to Midnight network capacity.

On-chain marketplace models

Beyond off-chain models, future protocol upgrades could enable a larger, trustless, self-organized on-chain capacity marketplace, further expanding on the off-chain models described above.

- **Ledger-native capacity leasing:** once ledger-native capacity leasing functionality is available, NIGHT holders would be able to delegate lease management and payment collection to a ledger-native mechanism. Brokerage models could leverage this capability to manage leasing, opening up a path to a multichain, multi-asset Treasury.
- **On-chain capacity exchange:** the same protocol capability could enable the spot purchase of unused DUST generation via an exchange interface. Exchanges could provide matching and coordinate payments, while the on-chain protocol mechanism would minimize the level of trust required.

In both cases, the required protocol-level capability could potentially carry a built-in fee to support the Midnight Treasury. This fee would create new revenue streams for the network and deepen the integration between Midnight and the broader Web3 economy.

Efficient capacity pricing

An evolving capacity marketplace would allow for ever more efficient price discovery based on the efficiency and convenience of each solution, enabling service specialization within and outside the Midnight network. Intermediated solutions, like Babel Stations and exchanges, can potentially support fiat transactions, providing an entry point to convert fiat currencies into stable tokens.

Diversified Treasury

The Midnight on-chain Treasury will initially be funded exclusively with NIGHT tokens – first from the initial token distribution, and subsequently with a portion of block production rewards, as described in the block production section. The on-chain capacity marketplace could transform the Midnight economy by expanding the scope and reach of the Treasury.

A fee levied on capacity leased or purchased with non-NIGHT tokens via protocol-level on-chain mechanism would go to the Midnight Treasury. This design would enrich and diversify the Treasury to include multiple types of assets and assets across different blockchains. Fees collected outside of the Midnight network would be under the control of the Treasury, further underpinning the value of NIGHT as a Treasury-backed token. This would have the effect of not only strengthening the long-term sustainability of Midnight, but of creating deeper interconnection across blockchains.

Expanding network reach: multichain

Beyond the multi-resource consensus system that allows Midnight to tap into Cardano's robust proof-of-stake layer to secure the network while bootstrapping, the Cardano Partner Chain framework brings other features to enable the vision of a truly multichain future: cross-chain observability and multichain signatures.

Cross-chain observability

With cross-chain observability, when a user performs an action on one chain, it is possible to trigger an agent that can act on another chain. This functionality underpins the future development of cross-chain use cases, such as on-chain capacity exchanges.

For example: a user would like to execute transactions on Midnight and pay with ETH on Ethereum. The user would lock ETH on Ethereum and leverage cross-chain observability to access the capacity to execute transactions on Midnight via a cross-chain agent. In this scenario, the ETH payment via the capacity marketplace would be split between the capacity (DUST resource) provider, the cross-chain observer, and the Midnight Treasury (via fee on the protocol-level function).

Multichain signatures

Multichain signatures allow Midnight-managed Treasury to receive inflows of fees from such on-chain services denominated in other tokens, building up diverse reserves in smart contracts native to their respective blockchains.

5. Block production and incentives

A core utility of NIGHT will be to incentivize Midnight block producers to build and validate new blocks on the network.

Block production at launch

Block production plays a fundamental role in the security of a blockchain – and, consequently, in the broader utility and value for all network participants. It is also where many networks are most vulnerable in their early days, when the incentives at stake are not yet established and can be exploited by potential attackers.

To mitigate that risk, the task of producing blocks and securing the network at launch will be performed *exclusively* by a set of trusted *permissioned nodes*, with a view to progressively decentralize, open up, and become fully permissionless. These initial block producers **will not receive block production rewards**.

Moving toward permissionlessness

In time, as per the Cardano Partner Chain framework, this progressive decentralization will open up consensus participation to those Cardano SPOs who choose to also take on a role as Midnight block producers, thus becoming eligible to receive block production rewards.

Depending on factors that will not be known until after mainnet is operational, the transition to a fully permissionless system may involve a gradual process with an intermediary, hybrid stage. During this stage, both permissioned nodes and participating SPOs acting as Midnight block producers would work alongside each other to validate Midnight blocks.

Cardano SPOs and Midnight block production

When the expected developments in the Midnight mainnet allow, the role of producing blocks will require that prospective Midnight block producers be Cardano SPOs. To be considered an eligible candidate for block rewards, a Cardano SPO will have to register with a unique smart contract on Cardano that oversees the Midnight block production candidate pool. NIGHT block rewards will be tallied and made available for withdrawal, on the Midnight ledger, by participating SPOs and the delegators whose stake enables those SPOs' block production.

Becoming a Midnight block producer will not interfere with an SPO's capacity, probability of being selected to validate Cardano blocks, or receiving ADA rewards for their contribution to Cardano security. There will be no impediments to performing roles in both networks. SPOs acting as Midnight block producers will be selected in proportion to their delegated ADA stake. Delegated ADA will not move and will remain under control of their holders on Cardano.

NIGHT block rewards, when operational, will be issued to each block producer's designated address(es) on the Midnight network, according to the rules and principles outlined below.

Producing Midnight blocks

As part of the Substrate framework³, the Midnight network plans on leveraging Grandpa⁴ (GHOST-based recursive Ancestor Deriving Prefix Agreement) to determine which blocks are finalized and AURA⁵ (Authority Round) to determine who produces the next block, using a round-robin system where validators take turns producing blocks at regular time intervals. The process will work as follows:

1. **Epoch distribution snapshot:** at the beginning of each Midnight epoch, a snapshot of the global stake distribution across candidates during the previous epoch will be taken to determine the current total active stake.
2. **Committee formation and slot leader election:** a committee of n block producers (where n is a configurable committee size system parameter) will be selected from the pool of all eligible candidates and assigned to lead random slots. Their stake weighs the probability of being selected to ensure representation is proportional to stakes.

Block rewards and the Reserve

Block producers process transactions according to protocol rules to achieve consensus over the network's state, thus maintaining its integrity. The more participants and the more resources that are deployed towards consensus and block production, the higher the overall resilience and security of the system. The Midnight protocol uses NIGHT to incentivize participants to perform these crucial tasks.

The NIGHT supply is minted at the outset of the token distribution. This supply includes all tokens – including those earmarked for block rewards, which are kept in the on-chain Reserve and out of circulation. The Reserve is managed by the Midnight protocol itself, and tokens therein are used for block rewards.

Moreover, block rewards come exclusively from the Reserve. Unlike many other blockchains, no new tokens are minted and no NIGHT-denominated fees are paid during transactions. Midnight transactions fees are paid in DUST (which by its non-transferrable and decaying nature cannot function as an economic incentive). This system ensures sustainable operations: for users, there is no recurrent capital expenditure for merely transacting on Midnight (given that DUST is a renewable resource), reducing operational costs and the accounting burden that would ensue.

Finally, the distribution of block rewards is inextricably connected to – and a function of – the Reserve, as detailed below.

³ <https://docs.polkadot.com/develop/parachains/intro-polkadot-sdk/#substrate>

⁴ <https://github.com/w3f/consensus/blob/master/pdf/grandpa-old.pdf>

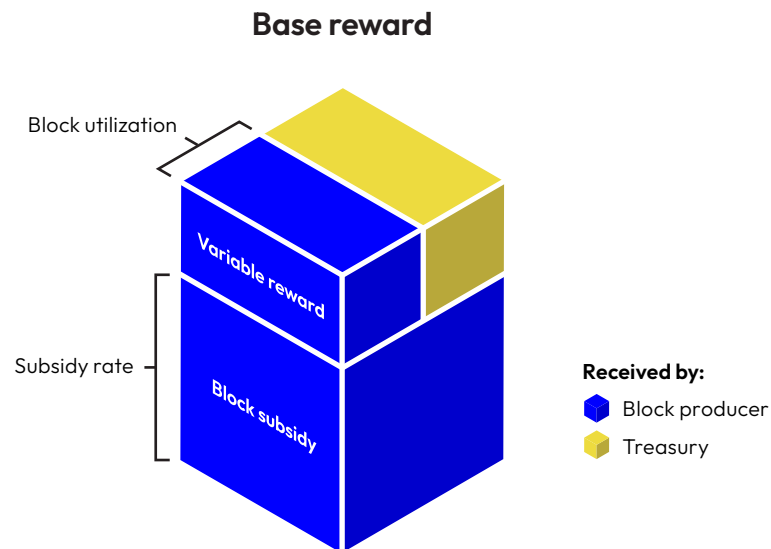
⁵ <https://openethereum.github.io/Aura.html>

Understanding Midnight block rewards

Midnight block rewards are dispensed by a dedicated, protocol-managed token Reserve, based on a constant *base distribution rate* that is used to calculate the *base reward* – the amount of tokens distributed at each block. While the rate is constant (in relation to the Reserve), the number of distributed reward tokens decreases with each new block as the number of tokens in the Reserve decreases. This pattern forms a decreasing curve that, in practice, means that the Reserve can last for a very long time (in the order of hundreds of years).

To incentivize efficiency in transaction processing, each base reward is further divided into a *fixed subsidy* and a variable *component* based on *block space utilization*. The ratio of the split is defined by the *subsidy rate*, a protocol-level system parameter.

The fixed subsidy is distributed entirely to block producers, while the variable part of the reward is split between block producers and the on-chain Treasury according to the “fullness” of the block. The “fuller” a block is, the larger the share of variable reward that goes to the block producer. These mechanisms are described in detail below.



Block rewards distribution

Block rewards are distributed as a *fixed* percentage of the remaining NIGHT held in the Reserve at each block. This percentage corresponds to a system parameter called the *base distribution rate* (more on this below). As the number of outstanding tokens in Reserve decreases with every block reward, this mechanism translates to a smooth, decelerating distribution curve. To illustrate how this works, imagine a theoretical example where the Reserve allocation is 1,000 tokens, of which the protocol distributes 10% of the remaining tokens with each block. From there, the example progression goes:

1. Block T: 1000 starting tokens, 100 tokens distributed as rewards;
2. Block T+1: 900 starting tokens, 90 tokens distributed as rewards;
3. Block T+2: 810 starting tokens, 81 tokens distributed as rewards;
4. (...) and so on, decelerating at each step.

Using this method brings several benefits:

- **Simplicity:** the baseline distribution of rewards can be easily adjusted via a single parameter: *the base distribution rate*.
- **Predictability:** at any point in time, block producers can calculate the amount of rewards they will receive based on their relative stake, and the community can confidently estimate how long the Reserve will last
- **Sustainability:** rewards decrease with every block, following a smooth, tapering curve pattern that means that the Reserve would not be depleted for hundreds of years, in most cases (depending on the initial allocation).

Base distribution rate

The *base distribution rate* (R) is a system constant that expresses the percentage of outstanding Reserve tokens that are distributed at each block (or, to put it another way, the share of tokens that leaves the Reserve with each passing block). The initial value of R can only be determined after the token distribution ends and NIGHT allocations are defined, and it is fundamentally a function of the following parameters:

- The percentage of tokens allocated to both the *Reserve* (B) and *Treasury* (T) (in relation to the total supply) at the end of the token distribution period;
- An *initial inflation rate* for the circulating supply – that is, the initial rate at which tokens enter into circulation with respect to NIGHT already in circulation.
- The network's *blocktime* (t), the average time it takes for block producers to produce one block in the network (in seconds).

The initial (annual) inflation rate on Midnight is set at π . This value is lower than the initial expansion rates observed on Ethereum (5%) and Cardano (7%), and it is close to what most economists consider a [healthy inflation rate](https://www.federalreserve.gov/faqs/economy_14400.htm)⁶. It should be stressed that the use of the term “inflation” here is relative to the expansion of the circulating supply. Tokens merely move from the Reserve and into circulation via block production rewards. This initial rate decreases with time, as fewer tokens enter circulation at each block relative to the ones already circulating.

The network's blocktime (the number of seconds it takes to produce one block) is not yet determined, as Midnight is still undergoing tests and optimization. The *actual* block time is bound to vary until the Midnight mainnet is deployed. Even then, as the protocol evolves, blocktime may change to reflect advances in technology or community decisions. At mainnet launch, it is expected that the network's blocktime will sit *within the range of one and ten seconds (1 to 10s)*. This value will determine the number of blocks produced in a year (γ).

⁶ https://www.federalreserve.gov/faqs/economy_14400.htm

Calculating the base distribution rate

Given that the inflation rate is expressed in annual terms, to solve for the *base distribution rate* (R) per block, one must first solve for the *annual base distribution rate* (R_a):

$$R_a = \frac{\pi(1 - B - T)}{B}$$

Where R_a represents the percentage of tokens dispensed from the Reserve to match the inflation of the circulating supply set at π during the first year. The precise value of R_a is a system parameter codified in the Reserve smart contract.

From there, the base distribution rate per block can be calculated by dividing R_a by the number of Midnight blocks (γ) produced in a year:

$$R = R_a \div \gamma$$

Base reward

The base distribution rate is then used to determine the *base reward* (N_b) for each block – that is, the total number of tokens distributed as rewards at each block – by simply multiplying the current *outstanding number of tokens in Reserve* (B_o) by R :

$$N_b = B_o \times R$$

Incentivizing full blocks

Since DUST is not transferable and does not function as a store of value, a challenge emerges: incentivizing block producers to include transactions in their blocks rather than opting to produce empty blocks (which would undermine the network's functionality and value).

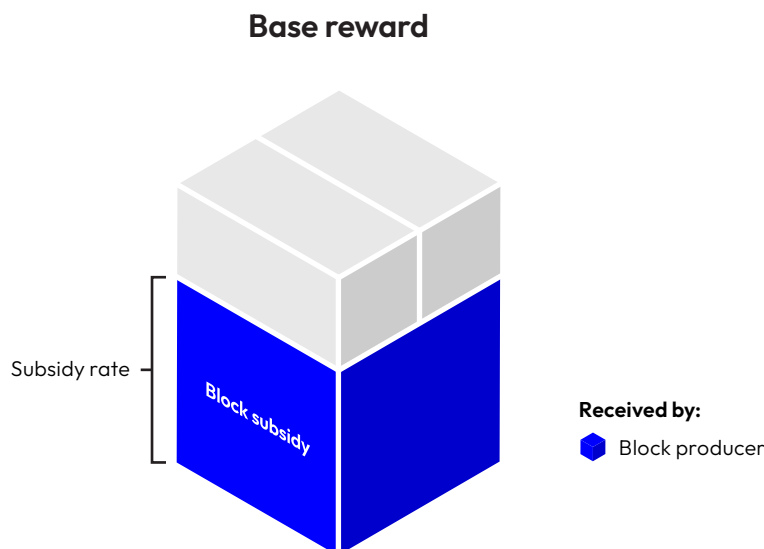
To address this issue, the base reward is split between a *fixed subsidy* and a *variable component* based on block utilization. The ratio of the split is determined by a *subsidy rate* (described below).

The *fixed subsidy* component ensures that block producers receive a baseline incentive for each block they produce, regardless of the block's fullness.

The *variable* component is designed to incentivize block producers to include as many transactions as possible in their blocks (as measured by utilized block space), increasing the network's efficiency and utility. Block producers receive variable reward in proportion to how "full" the produced block is; the remaining part – corresponding to the block's non-utilized space – is received by the on-chain Treasury.

Subsidy rate

The *subsidy rate* (S) is a system parameter that expresses the proportion of the base reward that is distributed to block producers irrespective of block utilization.



For example: a subsidy rate at 80% means that, for any given block, 80% of the NIGHT base reward is received by its producer, even if the block is empty. The remaining 20% – the variable reward component – is split between the block producer and the Treasury in proportion to block space utilization (see below).

At launch, the value of the subsidy rate is set to 95%, on the high end of the spectrum, to ensure that early block producers are incentivized to participate, while accounting for the fact that reaching peak adoption and demand for block space may take time. This high value also minimizes the incentive for block producers to stuff blocks with their own transactions and in doing so, raising DUST utilization. The subsidy rate can be adjusted via governance action: in the future, it is expected that it will be adjusted towards 50% so that block producers have a stronger incentive to create full blocks, thus increasing the overall efficiency of the system.

Calculating the block subsidy

One can determine the *fixed block subsidy* (N_f) of a given block by simply multiplying the base reward by the subsidy rate:

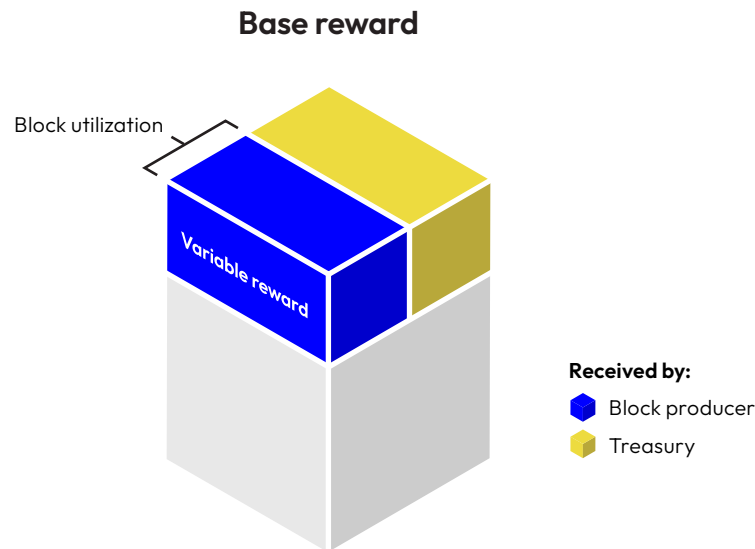
$$N_f = N_b \times S$$

The block subsidy is received entirely by the block producer. The difference between base reward and block subsidy corresponds to the *variable reward* (N_v).

For example: if the subsidy rate is set at 80%, then four-fifths of a block's base rewards are received by its producer – even if the block is completely empty. The remaining 20% make up the variable reward.

Variable reward

The *variable reward* (N_v) received by block producers corresponds to the difference between the base reward and the fixed block subsidy, weighed by each block's *utilization ratio* (U) – the percentage of block space that is utilized with respect to the maximum possible block size. The value of U depends solely on transaction dynamics and network usage; the higher a block's utilization ratio is, the larger a share of the variable reward goes to that block's producer.



Calculating the variable reward

Calculating the *variable component* (N_v) of the block reward requires one to simply multiply the block utilization rate by the difference between base reward and block subsidy.

$$N_v = U \times (N_b - N_f)$$

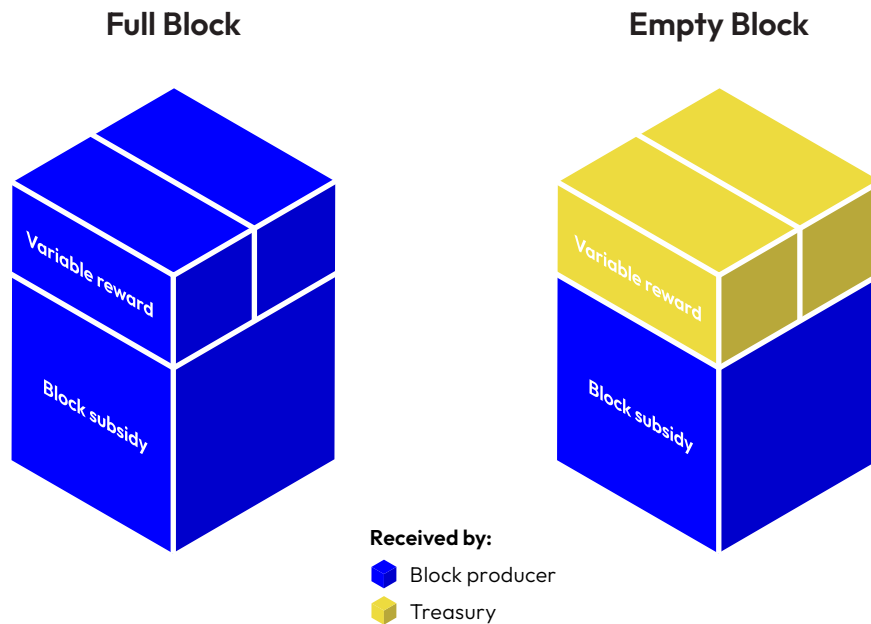
Following the previous example: the remaining 20% of the base reward is dispensed in proportion to how full the block is. If the block is completely full, the producer receives the full amount (i.e., 20% of the base reward); if the block is only 50% full, then the producer receives only half of the variable part (i.e., 10% of the base reward). The remaining half (the other 10%) goes to the Treasury.

Actual reward

For any given block, the *actual reward* (N_a) received by the block producer is the sum of the fixed and variable components, and it cannot be higher than the base reward for that block.

$$N_a = N_f + N_v$$

For a full block, the actual reward is *equal* to the base reward; conversely, for a completely empty block, it is equal to the fixed block subsidy.



Note that the actual reward can, and most likely will be, lower than the base reward, as completely full blocks should not be the norm (that would be a sign of network congestion). Summing up the example above, given a *subsidy rate* of 80% and a *block utilization rate* of 50%, the producer would receive 90% of the base reward for that block.

Treasury share

Whatever is left from the block reward (corresponding to the share of non-utilized block space) is sent to the *Treasury share* (N_t).

$$N_t = N_b - N_a$$

Summary: calculating block rewards

In summary, the steps to determining block rewards are:

1. Determine the *base distribution rate* (R), based on the proportion of tokens allocated to the *Reserve* (B) and *Treasury* (T), (π as annual inflation rate, and γ as number of blocks produced in a year) by the end of the initial token distribution, in relation to the total supply:

$$R = \frac{\pi (1 - B - T)}{B}$$

2. Determine the *block's base reward* (N_b) by multiplying the *current outstanding tokens in the Reserve* (B_o) by the *base distribution rate* (R):

$$N_b = B_o \times R$$

3. Accounting for *subsidy rate* (S) and *block utilization* (U), determine the shares of the base reward – *the actual reward* – that go to block producers (N_a) and Treasury (N_t):

$$N_a = N_b \times [S + (1 - S) \times U]$$

$$N_t = N_b - N_a$$

4. Update the outstanding number of tokens in the Reserve (B_o) to account for the distribution of that block's base reward (N_b).

This system achieves a fully predictable distribution of rewards, split between block producers and on-chain Treasury, while at the same time incentivizing maximum transaction inclusion within a block.

6. NIGHT token distribution

Note on tense and realized outcomes. This section records the NIGHT token distribution as designed. The Glacier Drop and Scavenger Mine claim phases have concluded; the Redemption Period commenced on 10 December 2025. The Midnight genesis block was produced on 17 March 2026 at 03:17:00 UTC, and the official production mainnet chain was launched on 30 March 2026. The Lost-and-Found claim phase will commence sometime after Midnight mainnet launch. Realized final allocations across all buckets are summarised in the “NIGHT token allocation” subsection below.

The initial distribution of the native crypto asset that grants access, utility, and control over the network is a fundamental component of any blockchain system. In the case of Midnight, this asset is the NIGHT token. The values and attributes of this distribution are a precursor to, and exert a strong influence on, the long-term future of any project; therefore, it’s crucial that they reflect the values and vision behind Midnight. The distribution of NIGHT tokens is designed to be:

- **Broad:** the NIGHT distribution shall empower a broad community with the means to access, operate on, and contribute to Midnight. No single party or group shall exert overwhelming influence over the network.
- **Inclusive:** the distribution shall be open to participants from Web3 and beyond, ensuring diversity on the network and establishing mutual interest and support between ecosystems.
- **Participative:** the community shall have an active role in claiming the token supply and helping originate and seed the core constituents needed to operate the Midnight network.
- **Free:** tokens shall be allocated to the community of eligible participants at no cost.
- **Accessible:** the claims process shall be simple and clear, and it shall give the community time to place their claims and redeem their tokens.
- **Transparent:** The source code for smart contracts governing the operation of the distribution will undergo a comprehensive third-party security audit and shall be published and open-sourced.

Process overview

The NIGHT token distribution consisted primarily of three claim phases and a redemption period. (the third claim phase – Lost-and-Found – will commence sometime after Midnight mainnet launch).

- **Claim phase 1:** In the first phase, the *Glacier Drop*, 100% of the total supply will be allocated to claims by the community of eligible participants based on criteria outlined in the corresponding subsection below. To broaden its reach and make up for the fact that, historically, token drops have had low participation, the Midnight token distribution implements two additional phases.
- **Claim phase 2:** The second phase, *Scavenger Mine*, will allow any prospective participant to play a role in the process of originating and seeding Midnight’s core network constituents by providing computing power to solve computational tasks aiding in the launch of the network. During this process, 100% of the unclaimed tokens from the Glacier Drop phase will be processed and apportioned between participants, core network constituents, and the third claim phase, as described below.

- **Claim phase 3:** The third and final claim phase will take place at a future date, following the launch of the Midnight mainnet on 30 March 2026: *Lost-and-Found*. Eligible Glacier Drop participants will be given another chance to claim a fraction of their original allocation.
- **Redemption period:** To complete the process and receive their NIGHT token allocations claimed, successful claimants will also have to redeem them – i.e., transfer them from a redemption smart contract to an eligible destination address supplied when making their claim.

The distributed nature of the token distribution’s technical setup means that the process will be run and validated by a group of multiple organizations and entities, strengthening the decentralization and security of the entire process.

Participants’ liabilities

The distribution of NIGHT tokens is not intended as a form of payment and has no implied real-world value (other than future application for chain utility). The distribution does not involve the sale of NIGHT tokens or the raising of proceeds. Eligible participants must accept the terms and conditions of the distribution in order to complete the journey and redeem their allocated NIGHT tokens. All legal and tax implications associated with the distribution’s activities are the participants’ sole responsibility, according to their jurisdiction and specific situation.

Claim phase 1: Glacier Drop

Duration: 76 days (5 August 2025 – 20 October 2025)

Overview

An evolution of the traditional airdrop formula, where tokens are merely dropped into eligible users’ wallets, the Glacier Drop includes mechanisms to increase its fairness, systemic integrity, and resistance to exploits by malicious parties. These mechanisms include the gradual *thawing* (unlocking) of claims, which inspires the *Glacier* part of its name.

Before the outset of the Glacier Drop claim period, eligibility will be determined and allocations calculated based on token balances in addresses across all participating networks. To mitigate the risk of exploits, a random date/time was selected — 11 June 2025, prior to publication of this paper — at which a snapshot of each participating network (Cardano, Bitcoin, Ethereum, XRPL, BNB, Solana, Avalanche, and Brave) was taken to determine eligible addresses and their NIGHT allocations. This random historical snapshot was used to mitigate insider information and reduce the risk of malicious parties gaming the distribution.

During Glacier Drop, claimed tokens are allocated to eligible claimants, but are initially *frozen* (locked) in a *redemption smart contract* on the Cardano network, and will not be transferable before they gradually *thaw* (unlock) during the Redemption period, as described in more detail below.

After Glacier Drop, the distribution then moves onto the second claim phase.

Eligibility

Initial eligibility to Glacier Drop is extended to participants in some of the most well-established Web3 ecosystems. Eligible ecosystems were selected for their contributions to the evolution of blockchain technology, decentralized applications, and to help build the Midnight ecosystem with a diverse and experienced community from the outset.

Individual eligibility is assessed on the basis of control over blockchain addresses within eligible ecosystems, using purely on-chain data; no personally identifiable registration is required, and no nonpublic personal information (NPI) is required to participate (although the option to sign up for a mailing list may be offered). The same person may claim using multiple qualifying addresses. Addresses may be eligible for the claim if they meet the following criteria:

1. **Eligible ecosystems:** addresses pertaining to any of the following networks/projects: Cardano, Bitcoin, Ethereum, Solana, XRPL, BNB Chain, Avalanche, and Brave. The same user may claim against multiple qualifying addresses.
2. **Minimum balance:** at the time of the snapshot, the address shall hold the equivalent value of at least 100 USD in native tokens of the respective network (ADA, BTC, ETH, SOL, XRP, BNB, AVAX, and BAT). Token prices will be assessed based on the rates on CoinMarketCap⁷ at the time of the snapshot. This mitigates potential Sybil attacks and similar bot activity exploits.
3. **Unsanctioned:** blockchain addresses matching those listed on the Specially Designated Nationals (SDN) list of the US Department of the Treasury's Office of Foreign Assets Control (OFAC) – based on assessment by a reputable blockchain forensics provider, such as Chainalysis – are not eligible for the claim.
4. **Community protection:** addresses that, as determined by the Midnight TGE, do not pose undue burden or harm to the Midnight community or its ecosystem.

Allocation sizes

During Glacier Drop, 100% of the total supply of 24 billion NIGHT tokens will be made available to be claimed by eligible addresses on a per-network, native-token-balance-weighted basis.⁹

Network allocations

The amount of NIGHT allocated to each network will be allotted as follows:

- 50% of the total supply allocated to Cardano participants
- 20% of the total supply allocated to Bitcoin participants
- The remainder of the total supply will be divided among the remaining qualifying networks in proportion to the relative USD value of the token holdings (as per CoinMarketCap data) of eligible participants at the snapshot.

⁷ <https://coinmarketcap.com/>

⁸ <https://www.chainalysis.com/>

⁹ Please note, it is beyond the realm of technical feasibility for the Midnight TGE or anyone else to guarantee that every eligible address corresponds to a human being who has the technical capacity to claim the allocated NIGHT.

Individual allocations

Individual allocation sizes will be weighed based on address balances captured by a historical snapshot of each network taken before the publication of this paper. The number of NIGHT tokens allocated to each participating address is determined as follows:

1. Let (S_j) be the number of NIGHT tokens allocated to a specific participating network (j) out of the total NIGHT supply (S) ;
2. Let (V_i) be the number of eligible native tokens that a single qualifying address (i) holds on that same blockchain network (j) ;
3. Then $(\sum V_i)$ is the total number of eligible native tokens held by all qualifying addresses on that network (j) ;
4. Then, the NIGHT token allocation (N_i) (denominated in STAR, the smallest subunit that makes up one NIGHT) to a qualifying address (i) on network (j) can be calculated using the following formula:

$$N_i = \frac{V_i}{\sum V_i} * S_j$$

5. Any remainder from this calculation will be left unclaimed and mined during the second phase;
6. Repeat steps (1) through (5) for each qualifying address on each participating network.

Mechanics: exercising claims

When the distribution window opens, the **NIGHT Claim Portal** – a website dedicated to claims – will be published. Detailed instructions on how to participate will be provided as each phase begins. Once the Glacier Drop claim period begins, eligible participants may exercise their claims by using that website to:

1. Demonstrate custody over their respective eligible blockchain addresses by signing a message using their private keys.
2. Provide an *unused* Cardano address (i.e., with no previous transaction history at the time of the claim) to serve as the destination address for receiving the redeemed NIGHT tokens. This is best practice and works to protect the personal data of claimants.

Tokens under third-party custody

Users whose tokens are under the custody of a third party (e.g., held by a centralized exchange or other custodian) will not be able to participate in Glacier Drop directly, as they cannot access the private keys needed to demonstrate ownership of qualifying assets. These users should contact their custodians to confirm whether they will support the NIGHT token distribution. Custodians may, at their sole discretion, choose to participate and distribute the claimed NIGHT tokens among those on whose behalf they hold assets in custody.

Auditability

Multiple measures are being taken to ensure the claim process is executed in the way that it is documented.

- **Code audit:** The source code of the smart contracts governing the operation of the distribution has been subjected to independent third-party security audits and has been published and open-sourced by the Midnight Foundation. The audit programme covering components in scope of, or directly relevant to, the NIGHT token distribution has been undertaken by TxPipe (Cardano-side smart contracts implementing the Midnight Protocol, including the NIGHT token Reserve, the upgradable-contracts library, and the Committee Bridge), Least Authority (core Midnight network components, including the Ledger, Indexer, Node and Midnight.js, the SHA-3 (Keccak) circuits within Midnight's zero-knowledge stack, and the Midnight Foundation Wallet SDK and DApp Connector API), TWEAG (Modus Create) (Cardano smart contracts used to execute the Glacier Drop NIGHT distribution and the design and documentation of Midnight's key-management and operational-security architecture), and Mandiant (a cyber-maturity and cloud-security assessment of the Midnight Foundation's production environments, together with an incident-response retainer, which engagement does not constitute a code audit). The Glacier Drop code base is published at <https://github.com/midnightntwrk/night-token-distribution>, and the Midnight Foundation maintains a public register of completed and in-flight audits accessible via the public repositories at github.com/midnightntwrk.
- **Data integrity:** A clear chain-of-custody (using digital signatures) process ensures claim snapshot data integrity, consistent with the defined steps and criteria.
- **Verification and proofs:** Submitted claims will undergo transaction correctness verification, through 100% committee consensus by multiple blockchain ecosystem operators (unaffiliated with the Midnight TGE). Proof of processing is recorded on the Cardano blockchain.
- **Censorship-resistance:** The process will be operated on chain via Cardano smart contracts.

1. Let S be the total supply of NIGHT tokens;
2. Let G be the number of tokens claimed during Glacier Drop;
3. Then, the share of unclaimed tokens from the total supply, available for processing and apportioning during Scavenger Mine S_u will be:

$$S_u = S - G$$

Phase rewards apportionment

The number of tokens from the Glacier Drop-unclaimed, carried-over tokens apportioned as rewards to participants in the Scavenger Mine phase will amount to a minimum of 1% of the total supply S , so that there is always a share of tokens available to Scavenger Mine participants. An equal number of tokens will be earmarked for the next claim phase, Lost-and-Found.

1. Let A_r be the total amount of tokens apportioned as rewards to Scavenger Mine participants;
2. Then, in relation to the total supply S , and to the tokens claimed during Glacier Drop G ,

$$A_r = \max\left(\frac{S}{100}, \frac{S}{10} - \frac{G}{2}\right)$$

3. And then, the corresponding total amount of tokens allotted to the core network constituents A_c will be:

$$A_c = S_u - A_r$$

The token supply available for core network constituents A_c will be apportioned among those as per the corresponding subsection below.

Individual allocations

Individual participants will be allotted a share of the NIGHT tokens apportioned on a daily basis as Scavenger Mine rewards in proportion to the amount of computational work units they complete out of the total number of work units completed by all Scavenger Mine participants in a given day. Individual allocations will be calculated as follows:

1. Given the total amount of tokens apportioned as rewards to Scavenger Mine participants in a given day A_r ;
2. Let C_m be the share of computation that a participant m provided in relation to total computation C on that given day;
3. Then, the number of tokens that a participant m will receive as reward R_m will be:

$$R_m = A_r \times \frac{C_m}{C}$$

Core network constituents apportionment

As part of the ecosystem origination and seeding mechanism, for every Scavenger Mine allocation to a participant, a share of the carried-over unclaimed Glacier Drop tokens will be apportioned to the core Midnight network constituents and to the third claim phase. This fundamental process is a function of the rate of claims during the Glacier Drop phase and it is executed as the Scavenger Mine draws to an end.

After Scavenger Mine rewards are accounted for, network constituents' share A_c will be distributed as follows:

Token Distribution	Constituent
$35\% \div A_c$	Midnight Foundation , a pool of NIGHT tokens will be allocated to supporting the growth of the ecosystem and its further development.
$30\% \div A_c$	Reserve ¹⁰ , a pool of NIGHT tokens held and governed autonomously by the Midnight protocol, whose only function is to issue block production rewards to block producers on the Midnight network.
$10\% \div A_c$	Midnight TGE , a pool of NIGHT tokens will be reserved for commercial partnerships to provide liquidity and support the growth of the network. Any allocated tokens not used for this purpose will be returned to the Reserve at a later date.
$5\% \div A_c$	On-chain Treasury , a pool of NIGHT tokens, stored in the ledger, belonging to the protocol and initially protocol-locked, with a view to being subject to the control of the decentralized on-chain governance mechanism that is expected to be developed, to fund ecosystem growth activities and projects that are selected via governance mechanics.
A_r	Lost-and-Found , claim phase token pool. The Lost-and-Found pool has been fixed at 192,600,598,491,058 STAR (0.8025% of total supply). This figure reflects the post-Scavenger Mine adjustments described under "Core network constituents apportionment" above — namely, the fixing of the Scavenger Mine participant pool at 1,000,000,000,000 STAR and the addition of 60,000,000,000,000 STAR to the Midnight TGE Ltd. allocation, each funded by a corresponding reduction of the pool originally earmarked for the Lost-and-Found phase. Accordingly, the Lost-and-Found pool is no longer equal to the tokens apportioned as rewards for Scavenger Mine participants, contrary to the formulaic position set out in the previous version of this whitepaper.

¹⁰ In case claims during Glacier Drop are such that the sum of all subsequent allotments surpass 100%, then the amount of tokens apportioned to the Reserve will be reduced by the excess amount.

For example: if 10% of the total supply are claimed during Glacier Drop, then, from the total allotment reserved to core network constituents during the Scavenger Mine phase, tokens will be apportioned as follows:

- **41.18%** to the Midnight Foundation;
- **35.29%** to the Reserve;
- **11.76%** to the Midnight TGE;
- **5.88%** to the on-chain Treasury;
- **5.88%** to participants in the Lost-and-Found claim phase;

Illustrative only. The actual final allocation following Glacier Drop and Scavenger Mine differed from this formulaic example by reason of the adjustments described immediately below; see the “Final NIGHT token allocation” subsection at the end of this Section 6.

Adjustments to formulaic apportionment

Following the conclusion of the Scavenger Mine claim phase, three adjustments were made to the formulaic apportionment described above so as to reflect realized participation and to maximise community access to NIGHT: (i) the Scavenger Mine participant pool was fixed at 1,000,000,000,000,000 STAR (i.e., $M = 1,000,000,000,000,000$ STAR); (ii) 60,000,000,000,000 STAR were added to the Midnight TGE Ltd. allocation; and (iii) the Lost-and-Found pool was correspondingly reduced. In addition, a non-divisible Scavenger Mine remainder of 873,988 STAR was allocated to the Reserve. The final allocations across all buckets are set out in the “NIGHT token allocation” subsection below.

Mechanics: exercising claims

To be eligible, participants must use the same NIGHT Claim Portal website as during Glacier Drop to:

1. Demonstrate successful completion of one or more computational tasks by providing cryptographic proofs of the solutions.
2. Provide an unused Cardano address (i.e., with no previous transaction history at the time of the claim) to serve as the destination address for receiving the redeemed NIGHT tokens. Participants who also took part in Glacier Drop can enter the same Cardano address they provided during the previous phase as long as it has no on-chain activity.

Like Glacier Drop, detailed instructions on how to participate in Scavenger Mine will be published on the NIGHT Claim Portal. The end of the Scavenger Mine phase will constitute the end of the period during which participants may claim tokens in the token distribution described in this whitepaper via the NIGHT Claim Portal.

Redemption period and thawing

Duration: 450 days

On 10 December 2025, the Redemption period began, during which each Glacier Drop and Scavenger Mine distribution thaws (unlocks) following a four-installment staggered schedule over the course of 360 days. The date of the first installment was randomly determined to fall over a range of 1-90 days), with subsequent installments following every 90 days. Token unlocks happen in equal 25% shares at each thaw.

This design mitigates the chances of supply shocks or sudden spikes in token flows that may distort supply-and-demand market dynamics, thus preventing manipulation of the token's circulating supply during the early days of the network.

The exact date of the first unlock depends on a random number that is generated and assigned to each claim upon successful submission of the claim before the Redemption period starts. For example:

- **A day-1 schedule** would unlock 25% of the tokens on days 1, 91, 181, and 271.
- **A day-25 schedule** would unlock 25% of the tokens on days 25, 115, 205, and 305.
- **A day-90 schedule** would unlock 25% of the tokens on days 90, 180, 270, and 360.

Any residual amounts (in case the number of tokens is not divisible by four) will be allocated to the last cycle. The thaw schedule count starts from 10 December 2025 (day zero), being the date on which the Redemption Period commenced.

Redeeming claims

Successful Glacier Drop and Scavenger Mine claimants may use the NIGHT Claim Portal to redeem their NIGHT tokens as they unlock, following the schedule outlined above. Claimants may choose to redeem each share of their allotted tokens as they thaw, or wait until their tokens fully unlock to redeem the whole allotment at once. Each transfer of NIGHT tokens from the redemption smart contract will require that the claimant pays a Cardano network fee (as described in the subsection below). At the beginning of the Redemption period:

- **NIGHT** tokens that have been claimed in the Glacier Drop and Scavenger Mine phases will become freely transferable as they thaw (unlock).
- **NIGHT** tokens allotted to the Midnight TGE and the Midnight Foundation will be immediately transferable and capable of being used in pursuit of advancing the development of the Midnight ecosystem.
- **NIGHT** tokens allotted to the Reserve will be held and controlled by the protocol itself, and will not be transferable except as block production rewards following the rules described in the corresponding section.
- **NIGHT** tokens allotted to the Treasury will be stored in the ledger, owned by the protocol, and initially locked, with a view to being unlocked when the expected on-chain decentralized governance mechanism for the Midnight network is implemented.
- **NIGHT** tokens claimed in the Lost-and-Found phase will not be subject to thawing (lockup) and will be immediately transferable.

Cardano transaction fees

NIGHT tokens are distributed for free. However, the redemption of Glacier Drop and Scavenger Mine claims requires that claimants execute a transaction on the Cardano network. Each such transaction incurs a nominal network transaction fee to be paid in Cardano's native token, ADA.

Cardano does not have a single, fixed transaction fee. Instead, the minimum fee for any given transaction is calculated using a formula defined by the protocol. For a typical simple transaction on Cardano, as of 9 April 2025, the minimum transaction fee was around 0.16 to 0.17 ADA – around USD \$0.09 as of that same date; the figure is illustrative of the fee level at that historical date and Cardano network fees may vary at the time of any given redemption. Further details on Cardano fees can be found at the [Cardano documentation website](https://docs.cardano.org/about-cardano/explore-more/fee-structure).¹¹

NIGHT Claim Portal sunseting

The Redemption period concludes with a 90-day grace period during which the NIGHT Claim Portal website will remain operational, allowing redemptions to continue beyond the thawing of the last tokens. Following this period, the NIGHT Claim Portal will cease to be operational, and participants in Glacier Drop and Scavenger Mine who have not yet redeemed their tokens will have to use their own means to interact with the smart contracts on the Cardano network to do so.

Claim phase 3: Lost-and-Found

Duration: four years (or until all remaining tokens are claimed)

Following the launch of the Midnight mainnet, giving original Glacier Drop-eligible participants (who did not claim during the initial 76-day claim period) another chance to claim a fraction of their original allocations. Participants claiming during this phase will have to use their own means to interact with the Midnight network smart contract that will hold their allocated tokens, and to submit and process their claims. Unclaimed tokens after the four-year period will be reallocated to the on-chain Treasury.

Eligibility

To be eligible for the Lost-and-Found phase, participants must have met all the eligibility criteria for the Glacier Drop phase and must not have claimed their allocations during the original Glacier Drop claim period.

Allocation sizes

Lost-and-Found allocations are a fraction of the original and are based on the same historical snapshots taken to determine eligibility for the Glacier Drop claim phase. The Lost-and-Found pool was set at 192,600,598,491,058 STAR (0.8025% of total supply), reflecting the post-Scavenger Mine adjustments described under “Core network constituents apportionment” above and summarised in the Final NIGHT token allocation subsection below.

¹¹ <https://docs.cardano.org/about-cardano/explore-more/fee-structure>

Phase allocation

The amount of tokens available for the Lost-and-Found phase will be the same as the amount distributed to participants in the Scavenger Mine phase.

Individual allocations

Lost-and-Found rewards will be calculated based on the size of the pool of Lost-and-Found tokens. Individual allocations will be apportioned in proportion to each claiming address's original Glacier Drop allocation in relation to the sum of all Glacier Drop-unclaimed allocations – using a transformation function to balance the distribution across the set of eligible addresses.

Mechanics: exercising claims

Participants will have to input proof of ownership of a Glacier Drop participating address to a smart contract hosted on the Midnight network. This proof will unlock the Lost-and-Found claim associated with that address, allowing the immediate transfer NIGHT to a destination Midnight address of their choosing. This transaction will be supported (paid) by DUST owned by the Lost-and-Found smart contract. No further support or resources – such as the NIGHT Claim Portal website – are anticipated to be provided to facilitate this phase.

NIGHT token allocation

All figures below are expressed in STAR, the smallest sub-unit of NIGHT. The conversion is fixed and protocol-enforced: 1 NIGHT = 1,000,000 STAR. Total supply = 24,000,000,000,000,000 STAR (equivalent to 24,000,000,000 NIGHT). STAR is used as the unit of disclosure because on-chain balances on the Cardano network (as a Cardano Native Asset) and on the Midnight network are denominated in STAR. To convert any figure to NIGHT, divide by 1,000,000.

Category	Allocation in STAR	% of total supply	Distribution status (as at 18 May 2026)	Vesting / unlock schedule
Midnight Foundation	8,400,000,000,000,000	35.0000%	100% unlocked / circulating	No protocol lockup; tokens immediately transferable from start of Redemption Period (10 December 2025).
Reserve	6,000,000,000,873,988	25.0000%	100% locked (protocol-controlled)	Locked until permissionless block production is enabled; thereafter released solely as block production rewards pursuant to Section 5 of this whitepaper. Includes the non-divisible Scavenger Mine remainder of 873,988 STAR.
Glacier Drop / Scavenger Mine - claimed	4,547,399,400,634,954	18.9475%	Partially unlocked (5 of 12 monthly tranches released; approximately 41.67% of pool unlocked as of May 2026)	Each successful Glacier Drop and Scavenger Mine claim thaws in four equal 25% tranches at days 1–90, 91–180, 181–270 and 271–360 from the Redemption Period start date (10 December 2025), with the first-tranche day randomly assigned per claim. Aggregate effect across all claims is a near-linear release over 12 months (December 2025 – December 2026), followed by a 90-day NIGHT Claim Portal grace period.
Midnight TGE Ltd.	3,660,000,000,000,000	15.2500%	100% unlocked / circulating	No protocol lockup; tokens immediately transferable from start of Redemption Period (10 December 2025). Reserved for commercial-partnership liquidity support; unused tokens to be returned to the Reserve at a later date.
Treasury (on-chain ecosystem)	1,200,000,000,000,000	5.0000%	100% locked (protocol-controlled)	Locked until decentralized on-chain governance is enabled; thereafter releasable only via on-chain governance proposals.
Lost-and-Found	192,600,598,491,058	0.8025%	100% locked pending launch of the Lost-and-Found claim phase	Tokens become claimable upon launch of the Lost-and-Found claim phase, which will commence sometime after Midnight mainnet launch. Once the phase has launched, eligible non-claimants from Glacier Drop have a four-year window to claim via direct interaction with the Lost-and-Found smart contract on the Midnight network. Claimed tokens are not subject to thaw and are immediately transferable. Any balance unclaimed at the end of the four-year window will be reallocated to the Treasury.
Total supply	24,000,000,000,000,000	100.0000%		

Figures reflect the post-Scavenger Mine adjustments described under “Core network constituents apportionment” above: (a) the Scavenger Mine participant pool was fixed at 1,000,000,000,000,000 STAR; (b) 60,000,000,000,000 STAR were added to the Midnight TGE Ltd. allocation; (c) the Lost-and-Found pool was correspondingly reduced; and (d) a non-divisible Scavenger Mine remainder of 873,988 STAR was allocated to the Reserve. Percentages are rounded to four decimal places. To convert STAR figures to NIGHT, divide by 1,000,000.

The NIGHT asset was created on the Cardano blockchain on 25 November 2025 (asset fingerprint `asset1wd3llgkhs6etxf2yca6cgk9ssrpva3wfOpq9a`). The current top holders of NIGHT, including the bucket-controlling wallets, are verifiable on the Cardano blockchain explorer at <https://cardanoscan.io/token/0691b2fecca1ac4f53cb6dfb00b7013e561d1f34403b957cbb5af1fa4e49474854?tab=topholders>. A labeled bucket-to-address mapping, which identifies each of the wallet addresses by allocation bucket, is maintained by the Midnight Foundation and is available at <http://midnight.gd/>

Holder concentration and conflicts of interest

Two entity-controlled allocations together represent a material concentration of supply that warrants express disclosure. The Midnight Foundation holds 8,400,000,000,000,000 STAR (35.0000% of total supply), and Midnight TGE Ltd. holds 3,660,000,000,000,000 STAR (15.2500% of total supply). Combined, the Foundation and Midnight TGE Ltd. hold 12,060,000,000,000,000 STAR — 50.2500% of the total supply of NIGHT. Both allocations were unlocked at the start of the Redemption Period on 10 December 2025 and are not subject to any protocol-level lockup.

The Midnight Foundation has discretion as to the transfer and use of the NIGHT tokens allocated to it. In addition to its token allocation, the Midnight Foundation currently operates two (2) of the thirteen (13) federated nodes that produce blocks on the Midnight network and contracts and pays the operators of the remaining federated validator nodes, and is a member of the governance committee described in the “Governance at launch” subsection above. In determining how to transfer or use the tokens allocated to it, or in carrying out its roles in relation to the current federated operation and governance mechanics of the Midnight network, the Midnight Foundation will act in accordance with its purpose of advancing the development of the Midnight ecosystem and with its own legal (including contractual) and regulatory obligations. In doing so, the Midnight Foundation may take decisions or actions that conflict with the interests of one or more other holders of NIGHT, or that favour the interests of one or more holders of NIGHT over others.

Midnight TGE Ltd. holds its allocation in reserve for use in commercial partnerships intended to provide liquidity and support the growth of the network. Allocations not used for those purposes are intended to be returned to the Reserve at a later date. In administering this pool of tokens, Midnight TGE Ltd. will comply with its legal and regulatory obligations with regard to conflicts of interest and the treatment of token holders.

Holders of NIGHT should be aware of this concentration and of the discretionary powers described above when making any decision in relation to acquiring, holding, transferring or otherwise dealing with NIGHT.

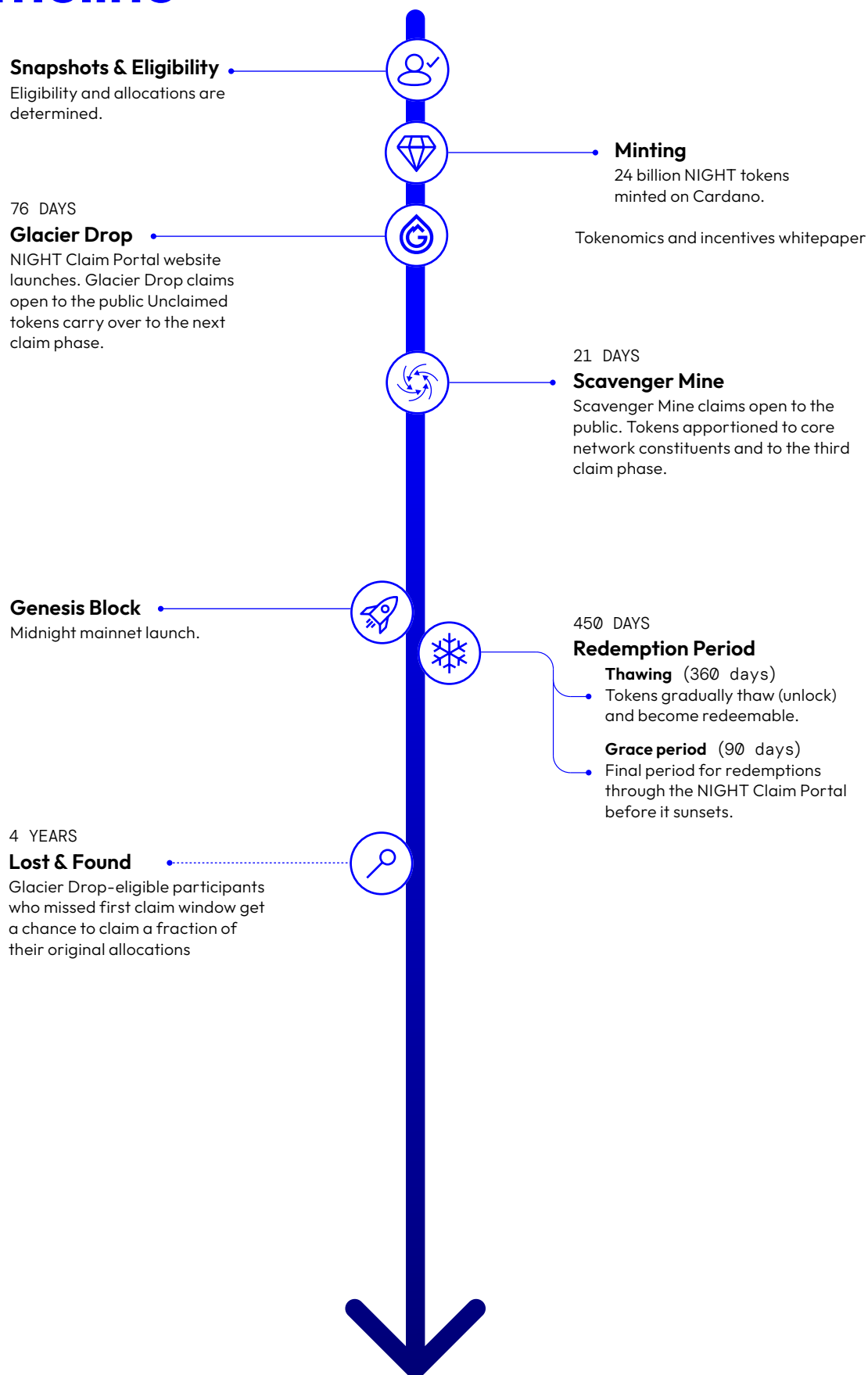
Custody, governance and movement attestation of entity-controlled wallets

The Cardano and Midnight network wallets controlling the Foundation and Midnight TGE Ltd. allocations are held under internal governance procedures established by, and applicable to, each entity. Those procedures provide for multi-signatory control of the wallets, with transfers requiring authorisation in accordance with the relevant entity's internal policies. The specific signing-key structure (including the multisig threshold and the identity or characterisation of signers) is held by the respective entity and is not disclosed in this whitepaper.

It is the present intention of the Midnight Foundation and Midnight TGE Ltd. to publish information from time to time regarding material transfers from the wallets controlling their respective allocations. This is a statement of present intent only and does not give rise to any contractual or other enforceable obligation owed to holders of NIGHT or to any other person.

Readers may verify on-chain balances held by NIGHT-controlling addresses, including the entity-controlled wallets referenced above, using the public Cardano blockchain explorer at <https://cardanoscan.io/> (search by Cardano NIGHT Policy ID 0691b2feccalac4f53cb6dfb00b7013e561d1f34403b957cbb5af1fa4e49474854) and on the Midnight network using the relevant Midnight network explorer. A labeled bucket-to-address mapping, which identifies each of the wallet addresses by allocation bucket, is maintained by the Midnight Foundation and is available at midnight.gd.

Timeline



7. Business Model

Core participants and Stakeholders

The Midnight ecosystem comprises four primary participant groups:

- **NIGHT holders**, who generate DUST — the network resource used to pay for transactions. See Section 3 (The DUST resource).
- **Midnight Block Producers (MBPs)**, who validate blocks and secure the network. Block production will gradually expand from the federated, permissioned set of trusted node operators in place at mainnet launch to participating Cardano Stake Pool Operators (SPOs) on a permissionless basis. See Section 5 (Block production and incentives).
- **DUST recipients, users and sponsees**, who use network capacity. Decentralized applications may sponsor users so that they can transact without holding NIGHT or DUST directly. See Section 4 (Cooperative tokenomics).
- **Midnight Foundation and on-chain Treasury**, which support ecosystem growth, ecosystem funding, and future decentralized governance. See Section 2 (The NIGHT token) under “NIGHT stakeholders” and “On-chain Treasury”.

Dual-token economy and shielded technology

Midnight separates asset ownership from transaction cost through a dual-resource model. NIGHT is the network’s core utility token; DUST is a non-transferable network resource generated by NIGHT and consumed to pay for transactions. This design allows users to interact with the network without expending their underlying NIGHT holdings.

Midnight uses zero-knowledge cryptography to support programmable privacy. DUST transactions are shielded by default, enabling private interactions while supporting compliance with applicable laws and regulations.

Governance and Midnight Improvement Proposals (MIPs)

Following the launch of the Midnight mainnet on 30 March 2026, the governance framework is expected to progressively decentralize through on-chain community participation. Once the framework is implemented, the community is expected to be able to (i) submit proposals through a Midnight Improvement Proposal (“MIP”) process, (ii) access on-chain Treasury funding through that process, and (iii) implement protocol upgrades approved through that process. The full specification and mechanics of MIPs are expected to be detailed in a future document.

Cooperative tokenomics: capacity-marketplace components

Midnight’s cooperative tokenomics architecture extends network access through a set of capacity-marketplace components, each of which is described in greater detail in Section 4

- **DUST leasing** — NIGHT holders may designate the DUST they generate to a Midnight address controlled by another party, enabling bilateral DUST-leasing arrangements outside the protocol layer.
- **Babel stations** — a planned mechanism through which users will be able to settle transaction costs using fiat currency or non-NIGHT digital assets via atomic-swap-style integrations.
- **On-chain capacity exchange** — a future on-chain marketplace, contemplated as a longer-term development, intended to permit trustless on-chain trading of unused DUST capacity.

- **Treasury revenue stream** — fees that arise from capacity usage and non-NIGHT payments are expected to accrue to the on-chain Treasury, supporting ecosystem sustainability and multi-chain growth, subject to the governance framework described above.

8. Roadmap

The four phases of Midnight’s development

Midnight’s development is structured across four phases (the “moon phases”), advancing the network from initial token launch toward a fully decentralized, interoperable privacy layer for the broader Web3 stack. Each phase reflects forward-looking aspirations of the Midnight Foundation as at the date of this whitepaper; the Legal Disclaimer on page 3 applies to all forward-looking statements in this section.

Phase 1 — Hilo (the first NIGHT) [completed]

- **Foundation and liquidity.** This phase established the network’s token supply and provided a testnet for builders to prepare real applications.
- **Token minting.** The total supply of 24 billion NIGHT tokens was minted natively on the Cardano blockchain as a Cardano Native Asset (CNA) on 25 November 2025, as verifiable on the Cardano blockchain explorer. See Section 6 (NIGHT token distribution) and the NIGHT token allocation subsection for the consolidated allocation as at the date of this whitepaper.
- **Distribution.** Through Glacier Drop (5 August 2025 – 20 October 2025) and Scavenger Mine (29 October 2025 – 19 November 2025), 4,547,399,400,634,954 STAR (equivalent to approximately 4.547 billion NIGHT) were claimed by the eligible community, laying the groundwork for subsequent secondary-market listings.

Phase 2 — Kūkolu (launching from a safe port) [current phase]

- **Genesis block and mainnet launch.** The Midnight genesis block was created on 17 March 2026 (genesis block timestamp 2026-03-17T03:17:00+00:00 UTC; genesis hash 0x1941ca8e2bb88146c14dea084d3be7eb6e96ca7135429c543848b628124f2854), and the Midnight mainnet was launched on 30 March 2026.
- **Federated era.** To support a stable and secure foundation for the first wave of privacy-enhancing decentralized applications, block production at mainnet launch is operated by a federated set of thirteen (13) trusted, institutional-grade node operators (of which two are operated by the Midnight Foundation and the balance by counterparties contracted by the Midnight Foundation) (see Section 7 (Business model)— Core participants and stakeholders).
- **Focus.** Deliver a stable Midnight mainnet operated by the federated set of trusted validators, supporting live privacy-first applications and use cases on the network.

Phase 3 — Mōhalu (broadening network participation) [target 2026]

- **Broader decentralization.** The network is expected to scale up the federated mainnet and transition toward a permissionless system, with Cardano SPOs progressively coming online as active Midnight block producers.

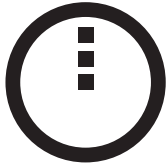
- **Scaled incentivized testnet.** The community is expected to be invited to actively validate and run the network alongside the federated mainnet, allowing prospective SPOs to test the system at scale.
- **DUST capacity exchange.** Development is expected to advance the on-chain marketplace through which NIGHT holders may trade or lease their generated private-transaction capacity (see Section 7 (Business model) and Section 4 (Cooperative tokenomics)).
- **Economic incentives and research and development.** Other expected 2026 developments include the Midnight DeFi Kernel, the Passport Programme for decentralized identity, and design work on a future consensus mechanism.

Phase 4 — Hua (emergence of hybrid dApps) [late 2026 and beyond]

- **Cross-chain interoperability.** Midnight is expected to transition from a stand-alone network into an interconnected privacy hub serving the broader Web3 ecosystem.
- **Hybrid dApps.** Through interoperability rails, developers are expected to be able to build applications operating across multiple chains.
- **Embedded privacy.** Midnight's programmable privacy and selective-disclosure features are expected to be capable of being embedded directly into existing applications on other ecosystems, without altering the native user experience.

9. Glossary

Term	Definition
Circulating NIGHT	All NIGHT tokens that do not belong to the Reserve (and thus, not considered uncirculated), including those belonging to the community and other core network constituents.
DUST	The shielded, renewable resource on the Midnight network that is used to access network capacity: its single function is to enable users to execute transactions on Midnight (transfers, smart contract interactions) while preventing network congestion.
Glacier Drop	The first phase – and sometimes also used as the namesake – of the multi-phase NIGHT token distribution. The Glacier Drop makes 100% of the total NIGHT token supply available to be claimed by eligible participants across the Cardano, Bitcoin, Ethereum, Solana, XRPL, BNB, Avalanche, and Brave networks.
Lost-and-Found	The third phase of the NIGHT token distribution.
NIGHT	Midnight's native token, whose primary function is to generate DUST, the resource that powers network operations. It will also be used for block production rewards, ecosystem growth incentives, and on-chain governance.
Proof-of-Stake / PoS	PoS is a consensus mechanism used in blockchain technology where users validate transactions on a network by "staking" a certain amount of cryptocurrency they hold. Midnight is a PoS-type blockchain.
Reserve	A pool of tokens that is reserved for payment of block production rewards. These tokens are considered <i>uncirculated</i> .
Scavenger Mine	The second phase of the NIGHT token distribution.
SPECK	One unit of DUST is further divided into one million subunits called SPECK.
Stake Pool Operator / SPO	A participant in a proof-of-stake blockchain network responsible for configuring and maintaining the node infrastructure that validates transactions, produces new blocks, and secures the network, often on behalf of other token holders (delegators).
STAR	One unit of NIGHT is further divided into one million subunits called STAR.
Treasury / on-chain Treasury	A pool of tokens that is reserved for ecosystem development purposes and is governed via on-chain voting.
Uncirculated NIGHT	NIGHT tokens held by the Reserve and earmarked for block production rewards.
Unlocked NIGHT	Unlocked NIGHT tokens can be moved by their holders and carry full utility.
Zero-knowledge / ZK	A cryptographic technique that allows one party to prove something to another without revealing any additional information. Zero-knowledge proofs (ZKPs) are used to verify information while keeping it private.

 **midnight**

Claim phase 2: Scavenger Mine

Duration: 21 days (29 October 2025 – 19 November 2025)

The second phase, Scavenger Mine, took place after Glacier Drop and before mainnet launch. It offered participants the opportunity to play a role in the process of originating and seeding Midnight's core network constituents, thus claiming a share of all unclaimed tokens from the Glacier Drop phase.

The Scavenger Mine phase will involve completing a computational task or puzzle, designed to be accessible to the general public and not favor mining companies. Scavenger Mine expands the NIGHT token distribution's eligibility requirements and gives the opportunity to an even broader swath of the internet to take part in the creation and future development of Midnight.

During Scavenger Mine, 100% of the tokens that were left unclaimed during Glacier Drop will be processed and apportioned. A share of the unclaimed Glacier Drop tokens will be allocated for claiming by Scavenger Mine participants, while the remainder will be apportioned to seed the core Midnight network ecosystem constituents – who are integral to the launch and operation of the network – and to the third claim phase.

The Scavenger Mine claim phase ran for 21 days. It was divided into 21 one-day slots, each beginning at 0:00 UTC. The pool of unclaimed tokens was split into 21 equal daily portions, and rewards were calculated and allocated at the end of each day.

NIGHT tokens claimed by Scavenger Mine participants will initially be frozen (locked) in a redemption smart contract on the Cardano network in the same fashion as Glacier Drop-claimed tokens. These tokens will be redeemable in the same manner – and subject to the same thawing schedule – as those claimed during Glacier Drop.

Eligibility

To be eligible to participate in the Scavenger Mine, participants must successfully complete and provide cryptographic proof of solution to computational tasks or puzzles requiring computing power. The puzzles will be carefully designed to ensure accessibility to the general public and prevent concentration of rewards among large mining operators.

Prospective participants do not need to have participated in (or meet the eligibility criteria set for) the Glacier Drop phase – although Glacier Drop participants are also welcome to participate in this phase.

Allocation sizes

During Scavenger Mine, 100% of the unclaimed supply of NIGHT tokens will be carried over from Glacier Drop to be processed and apportioned between Scavenger Mine participants, core network constituents, and the third claim phase. The share of the tokens apportioned to Scavenger Mine claimants and to each of the constituents is variable, and depend on the uptake of the first claim phase.