MORPHEUS.NETWORK

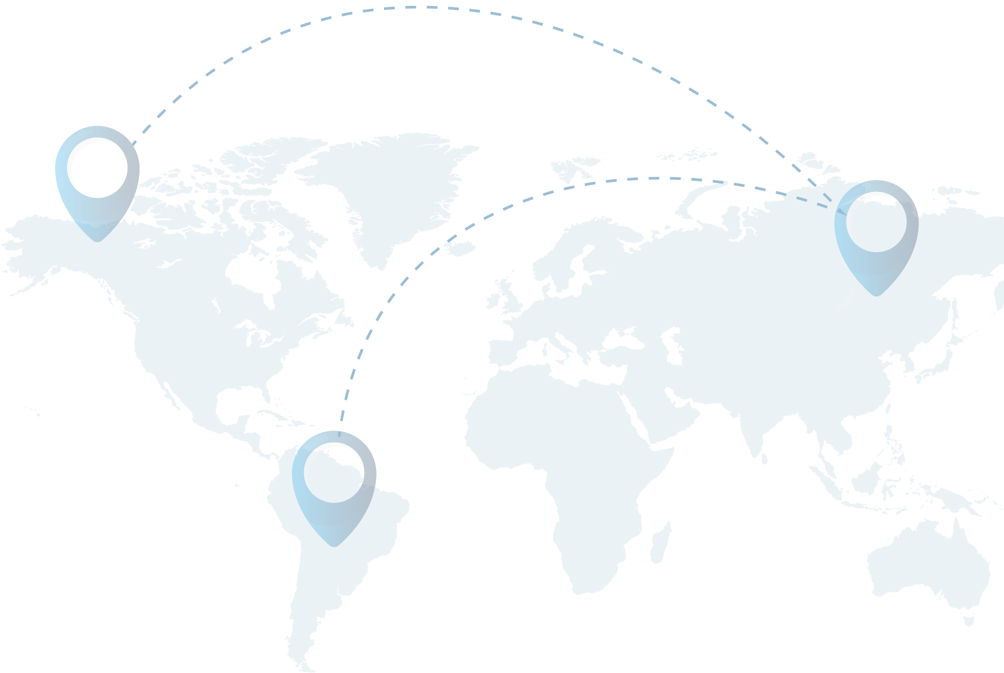
MORPHEUS.NETWORK'S TRUST.SUPPLY *MASTERNODES LIGHTPAPER*

UPDATED JULY 2025

Table of Contents

ABSTRACT

Morpheus.Network addresses global supply chain inefficiencies with middleware and blockchain-based solutions. This paper aims to highlight the network's overarching vision and the utility of its token and improved masternodes program. Traditional systems struggle with transparency, high costs, and slow processing. The MNW token and masternodes program optimize logistics and financial transactions by ensuring efficiency, security, and transparency. The masternodes program incentivizes participants to maintain full nodes, enhancing network stability, security, and functionality through transaction validation. Locking tokens as collateral creates a resilient decentralized validation network. Morpheus.Network's Trust.Supply system uses staked MNW tokens to ensure a comprehensive validation capacity, aligning validator incentives with network needs. Committed to innovation, Morpheus.Network aims to transform global trade by enabling connected, transparent, and sustainable supply chain management, setting new industry standards and driving progress for businesses worldwide.



Introduction

Morpheus.Network was founded in response to the growing complexities and inefficiencies in global supply chains. Traditional supply chain systems often suffer from issues such as lack of transparency, high transaction costs, and slow processing times. Recognizing the potential of blockchain technology to address these challenges, Morpheus.Network was established to create a more efficient, transparent, and secure supply chain solution. With a team of experts in logistics, technology, and finance, the company developed a comprehensive platform that leverages smart contracts and blockchain technology to automate and optimize supply chain processes. The introduction of the Morpheus.Network token ("MNW") and masternodes program further enhances the platform's capabilities, providing businesses with an even more powerful tool to manage their logistics and financial transactions

Motivating Vision

Morpheus.Network's mission is to transform the global supply chain and logistics industry through the application of advanced blockchain technology. The company is committed to providing a secure, efficient, and transparent platform that facilitates seamless financial and logistical transactions. The MNW token and masternodes program serve as the cornerstone of this initiative, further enabling businesses to streamline their operations, reduce costs, and enhance collaboration across the supply chain ecosystem.

- ***Morpheus.Network empowers enterprises of all sizes with the tools they need to optimize their supply chain management processes. By leveraging blockchain technology, the company aims to create an environment where businesses can achieve unparalleled efficiency, maintain compliance with regulatory standards, and ensure the highest levels of security for their operations. For more information about Morpheus.Network, please visit https://morpheus.network.***

TRUST.SUPPLY – THE PLATFORM

Overview

In the Trust.Supply system, validators are critical participants within a decentralized network that validates queries issued by various providers via the Trust.Supply API. Validators participate by staking MNW tokens, representing their commitment and capacity to perform validation tasks. The system ensures that demand for validation, indicated by the transaction count (TTT), is met by a robust supply of validator capacity, thereby aligning the incentives of validators with the needs of the network.

Masternode Approval Mechanism and Member Access to Portal

Individuals interested in participating as validators should begin by visiting the Trust.Supply Portal at https://trust.supply.

For masternodes, KYC is required to be passed before you can stake MNW tokens. You must also agree to the following terms: https://trust.supply/terms.

Note that there are certain regions referred to as "Prohibited Jurisdictions" in the terms above that are not able to participate.

KYC is performed via Sumsub.

You will need to provide government issued identification, ensuring the image quality is clear.

Once your KYC is approved you may need to pass a liveliness check via your phone.

You will then be notified via email if your KYC has passed successfully and can move onto staking to run masternodes via the dashboard.

Staking Mechanism

Validators stake MNW tokens to participate in the masternodes program, with each node requiring a specific amount of MNW tokens currently 1,800 MNW per node. This stake represents the validator's weight within the Equitable Validator Leader Selector (EVLS) algorithm, affecting its chances of being selected to validate queries.

Staking Terms and Rewards

Validators can choose to stake their MNW tokens for fixed terms of 3, 6, or 12 months (Calculated as N+1 days where N is the stake duration). The reward per validated transaction varies based on the term of the stake.

1. 3 months/90+1 days: 0.06 MNW per transaction
2. 6 months/180+1 days: 0.08 MNW per transaction
3. 12 months/365+1 days: 0.1 MNW per transaction

Validation Demand and Work Allocation

The Trust.Supply API determines the required number of validations per query, which varies depending on the provider and the type of information being validated.

Work Allocation Process

Each day, the EVLS algorithm selects validators based on their staked nodes to distribute the validation tasks evenly. The more nodes a validator has staked, the higher their probability of receiving work, promoting fairness and efficiency in task distribution.

Penalties for Early Unstaking

To maintain network stability and commitment, penalties for early unstaking are structured to discourage premature withdrawals while also adjusting rewards based on the completed duration of the stake relative to the committed term. All penalty fees will be added to the rewards pool.

Penalty Structure

1. Early Unstaking Penalty:
   Regardless of the term length or when the unstaking occurs, there is a flat penalty of 10% on the net rewards amount for unstaking before the end of the commitment period.

2. Reward Adjustments:
   Rewards are adjusted based on the last completed term prior to unstaking. Any partial term does not count towards reward calculations.

3. Cooling-Off Period:
   In the case of unstaking early, previously staked tokens and any accrued rewards will be held for 30 days before being returned to the wallet of origin.

Specific Scenarios and Calculations

1. **Example #1 :** Unstaking Before 3 Months (+1 day):
   1.1 Rewards: No rewards are paid.
   1.2 Scenario: A validator who stakes for any term but unstakes within 91 days forfeits all rewards.
2. **Example #2 :** Unstaking After 5 Months (6-Month Commitment):
   2.1 Rewards for Completed Term: Calculated at the rate applicable to a 3-month term (0.06 MNW per transaction).
   2.2 Penalty: 10% of the net rewards amount
   2.3 Scenario: If a validator commits to a 6-month term and unstakes at month 5, they receive rewards at the 3-month rate of 0.06 and a 10% penalty on the net rewards amount.
3. **Example #3 :** Unstaking After 10 Months (12-Month Commitment):
   3.1 Rewards for Completed Term: Calculated at the rate applicable to a 6-month term (0.08 MNW per transaction).
   3.2 Penalty: 10% of the net rewards amount.
   3.3 Scenario: If a validator commits to a 12-month term and unstakes at month 10, they receive rewards at the 6-month rate of 0.08 and incur a 10% penalty on the net rewards amount.

Term Definitions and Reward Rates

1. 3 months/91 days: 0.06 MNW per transaction.
2. 6 months/181 days: 0.08 MNW per transaction.
3. 12 months/366 days: 0.10 MNW per transaction.

Each term is effectively extended by one day to accommodate time zone differences and ensure clarity in term completion.

Uptime Requirements

Maintaining high availability is critical for the functionality of the network. Validators are required to ensure an uptime of 95% or higher for their validating software, which is typically run on Virtual Private Servers (VPS). This ensures that the network remains operational and capable of handling validation requests at all times, thereby maintaining its reliability and efficiency.

Daily Uptime Requirement

Immediate Consequences: Validators must meet the 95% uptime threshold daily to qualify for selection in the next validation day. Failure to meet this requirement results in the validator being ineligible for selection the following day, missing potential rewards. This slashing measure encourages validators to quickly address any issues that may affect their uptime.

Long-Term Uptime Requirement

1. End of Stake Term: If a validator's average uptime falls below 95% by the end of their staking term, they will forfeit any rewards accrued during that period. Instead of applying a penalty equal to the size of their stake, the forfeited rewards will be added to the rewards pool. These funds will then be redistributed in future validation cycles to other validators who meet the uptime requirements.
2. Opportunity for Recovery: Validators have the entire term to monitor and improve their infrastructure to ensure consistent uptime. Meeting the daily requirement consistently after any downtime is crucial to avoiding reward forfeiture at the end of the staking term.

Equitable Validator Leader Selector (EVLS) Algorithm

In distributed ledger technologies (DLT), maintaining decentralization and fairness in the validator selection process is crucial for system integrity and trust. The Equitable Validator Leader Selector (EVLS) algorithm addresses these challenges through a dynamically weighted random selection mechanism, where the selection probability is tied to the node count of each validator within the Validators Network. The algorithm includes measures to prevent monopolization by any single validator and ensures a balanced distribution of transaction validation opportunities.

Validators Network and Node Count Normalization

The Validators Network consists of a set of validators, each with an associated node count representing their weight in the selection process. Prior to initiating a validation cycle, we normalize the node counts to prevent any single validator from disproportionately influencing the network. This normalization process adheres to an anti-monopolistic guideline, ensuring that the node count of the largest validator does not exceed the sum of the node counts of all other validators in the network, multiplied by two, minus one.

Normalization Formula

Given a validators network $W = [w_1, w_2, ..., w_n]$ where w_i represents the node count for the i - th validator:

1. Calculate the sum of node counts for all validators except the largest:

$$Sum_{rest} = \sum_{j=1, j \neq i_{max}}^{n} w_j$$

**Here i_{max} is the index of the largest validator with the maximum node count.*

2. Adjust the node count of the largest validator (wi_{max}) if necessary:

$$wi_{max} = min\,(wi_{max}, 2\,x\,Sum_{rest} - 1)$$

Transaction Validation Cycles

The validation process is structured into cycles, each designed to handle a predefined number of transactions proportional to the total node count (SSS) of the normalized Validators Network.

Cycle Definition

Total Node Count (SSS):

$$S = \sum_{i=1}^{n} w_i$$

1. Number of Full Cycles (N) for a total of T transactions

$$N = \left[\frac{T}{S}\right]$$

2. Transactions in Last Partial Cycles (R):

$$R = T \bmod S$$

Each cycle involves a random selection of a validator based on the weighted probabilities derived from their node counts, followed by a decrement in the node count of the selected validator to ensure equitable participation across cycles.

Selection Process in the Equitable Validator Leader Selector (EVLS) Algorithm

Weighted Random Selection Mechanism

The EVLS algorithm employs a sophisticated method to ensure fair and unbiased selection of validators for transaction validation within the Validators Network. The selection process uses a weighted random selection mechanism, where the probability of a validator being chosen correlates directly with their node count after normalization.

Detailed Steps

1. Weight Assessment
   1.1. Each validator in the network is assigned a weight (w_i) that quantifies their stake or contribution to the system. These weights are indicative of the validator's capacity or reliability.

2. Total Weight Calculation
   2.1. The total weight (S) of all validators in the system is calculated as the sum of individual weights:

$$S = \sum_{i=1}^{n} w_i$$

   2.2. This total weight represents the entire 'weight' of the system and is used to scale the random selection process.

3. Cumulative Weight Computation
   3.1. Cumulative weights are computed to facilitate the selection process. For each validator i, the cumulative weight ($C(i)$) is the sum of all weights from the first validator to the i - th validator.

$$C(i) = \sum_{j=1}^{i} w_j$$

   3.2. These cumulative weights create thresholds that partition the weight into segments corresponding to each validator's contribution.

4. Random Selection Process
   4.1. A random number (r) is generated and scaled by the total weight (S), yielding a value in the range of 0 to S:

$$r = random\ (0,1)\ x\ S$$

   4.2. The selected validator is determined by finding the smallest index K such that:

$$r \leq C\ (k)$$

   4.3. This process ensures that the probability of selecting a particular validator is proportional to their weight.

Dynamic Adjustment of Node Count

Post-selection, the node count of the selected validator is decremented by 1:

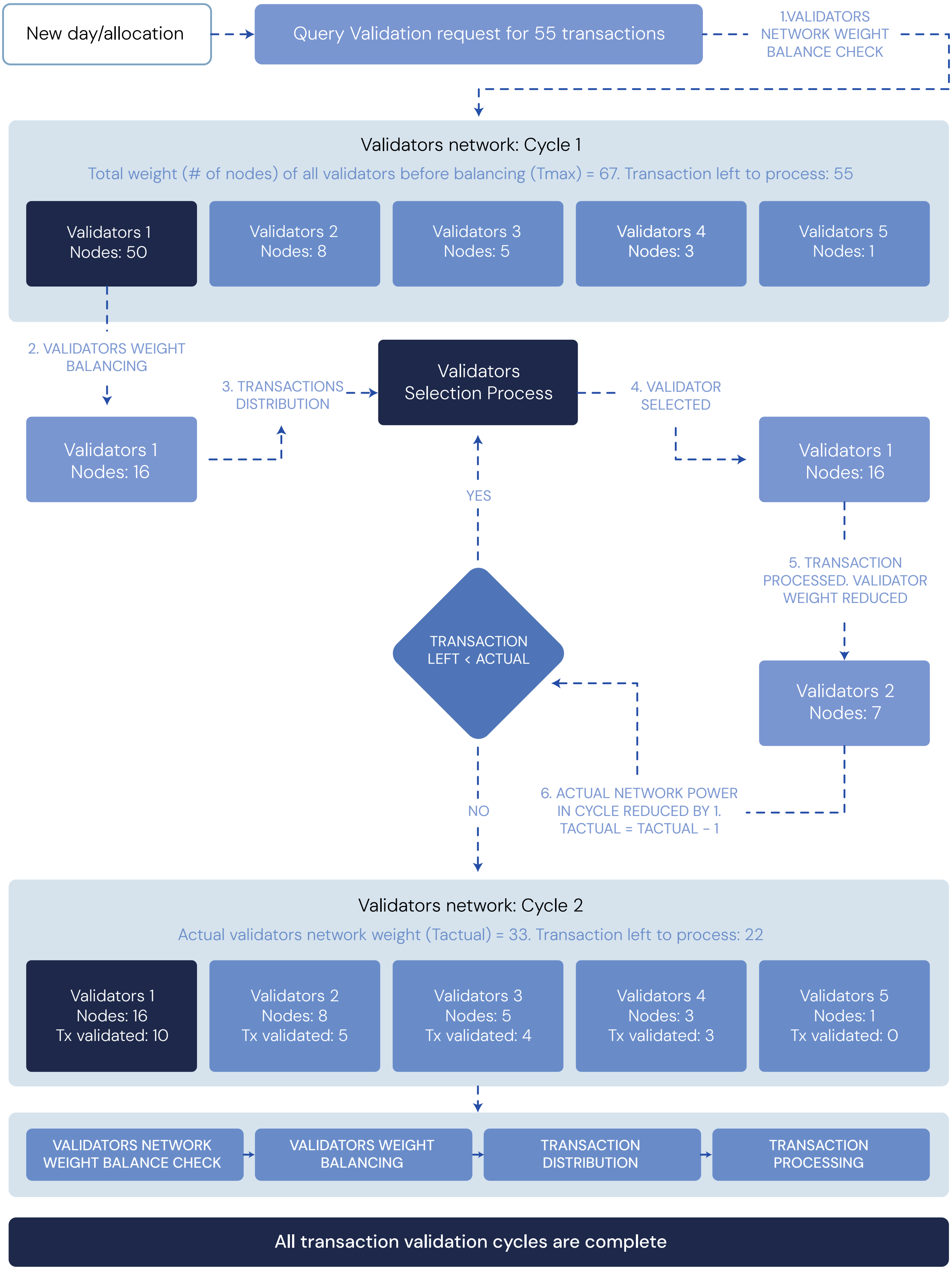
$$w_k = w_k - 1$$

This decrement is crucial as it dynamically adjusts the probability of subsequent selections, ensuring equitable participation across all validators. It prevents any single validator from repeatedly dominating the validation process due to a higher initial node count.

Monitoring and Adjustment

To maintain the integrity and efficiency of the selection process, continuous monitoring is conducted. Adjustments are made as necessary to ensure the algorithm remains adaptive to changes within the Validators Network, such as variations in node counts and the entry of new validators. This proactive approach ensures that the EVLS algorithm continues to perform optimally under varying network conditions.

EVLS Algorithm Example



Query Validation Process

Overview

The Query Validation Process is a core component of the Trust.Supply system, facilitating the validation of data queries issued by various providers such as IoT platforms, UPS, and SeaRates. This process ensures the integrity and accuracy of data through a decentralized network of validators, leveraging a robust response protocol to manage and verify the flow of information.

Validation Workflow

Query Distribution

Queries from different providers are received by the Trust.Supply API and entered into the Target Data Query Queue. Each provider's pool, for instance, the IoT Pool, UPS Validation Pool, and SeaRates Validation Pool have a specific demand and minimum confirmation requirement per query.

The total demand (as an example 56,000 queries for a given period) is managed by the validators network balancer, which distributes these queries based on the available capacity and stakes of validators.

Query Pickup and Validation

Queries are picked up from the queue by the balancer and distributed to the appropriate validation pool. For example, a UPS tracking query code might be distributed into the UPS pool.

Validators within the network (Node_1 to Node_N) pick up these queries for validation. The selection of validators for each query is determined by the Equitable Validator Leader Selector (EVLS) algorithm, which ensures that validators with higher stakes have a proportionately higher chance of receiving queries.

Validation Execution

Each validator executes the validation of the query using their resources. This involves verifying the data against predefined criteria or external data sources.

The raw responses from these validations are collected in the Raw Response Pool, where they are encrypted (e.g., SHA256 encryption) to ensure data integrity and security.

Response Handling and Blockchain Logging

The encrypted responses are evaluated, and a consensus mechanism determines if the responses meet the validation criteria.

Successful validations are logged onto the public blockchain, providing a transparent and immutable record of the validation process. This includes logging the response and the independent validation results, such as "5/6 validations matched."

Feedback and Update Mechanism

The validated queries map is updated with the results of the validations, and the Validators Network Balancer uses this information to adjust future query distributions.

This continuous feedback loop enhances the efficiency and accuracy of the validation process, ensuring that validators are effectively utilized based on their performance and reliability.

Query Validation Process