DYTALLIX

Quantum-Secure, Open-Source, Future-Ready

Dytallix Tokenomics White Paper

A Dual-Token, PQC-Native Economic Framework

Executive Summary

Dytallix establishes a strictly Post-Quantum Cryptography (PQC) native Layer 1 blockchain to address the systemic threat of Cryptographically Relevant Quantum Computers (CRQCs). Unlike hybrid architectures that retain classical vulnerabilities, Dytallix utilizes NIST-standardized lattice cryptography (ML-DSA, ML-KEM) for all consensus and transport operations.

The economic model utilizes a Dual-Token Architecture to decouple governance security (DGT) from transactional utility (DRT). This document formalizes the Dimensional Cost Function, which prices compute and bandwidth as independent vectors to mitigate the large footprint of PQC signatures, and the PID Emission Controller, which governs supply elasticity via control theory.

This specification unifies the cryptographic requirements of PQC with economic reality, addressing bandwidth OpEx, oracle dependencies, client-side computational burdens, and fair valuation through rigorous mathematical and logical mechanisms.

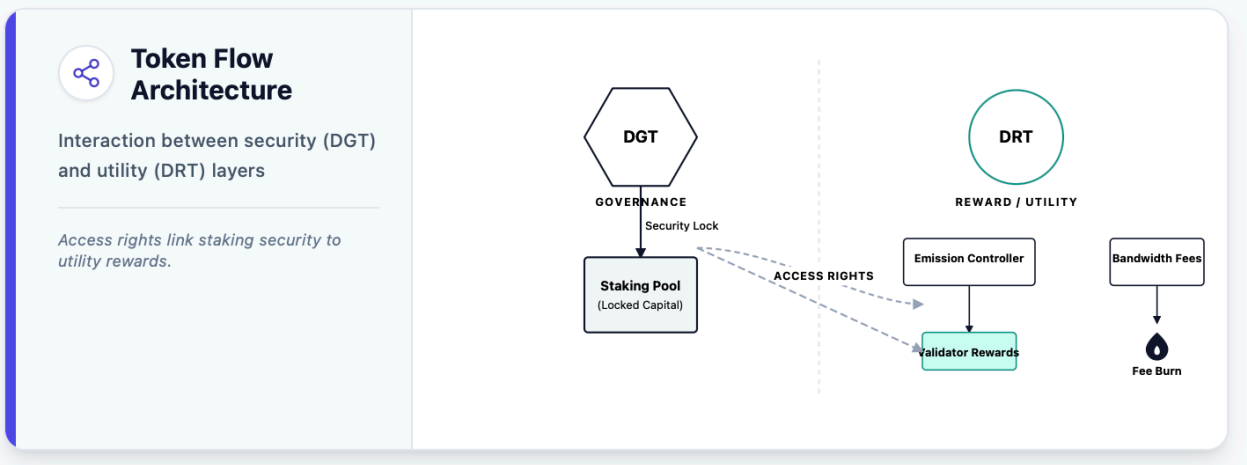
1. Scope and Non-Goals

To ensure clarity for implementers and auditors, this section defines the boundaries of this specification.

- **Core Protocol [Core Consensus]:** The Dual-Token Model, PID Emission Controller, Dimensional Gas Market, and Consensus Safety logic are critical consensus rules enforced by every node.
- **Modular Extensions [Module]:** The Oracle Medianizer, Gateway Fee Market, and Consul TEE are architected as enshrined smart contracts or sidecar modules. Their failure does not halt block production but may degrade economic efficiency.
- **Non-Goals:** This paper does not specify the precise P2P wire format (see Technical Whitepaper), the internal state trie structure (Sparse Merkle Trees), or the specific legal jurisdiction of the organization.

2. The Macro-Economic Model: Dual-Token Separation

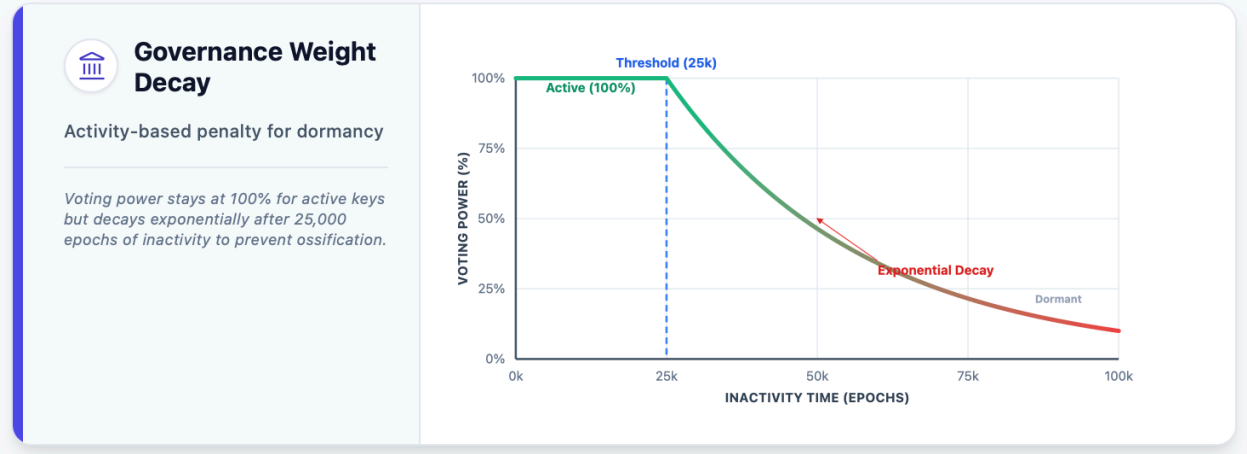
To resolve the economic trilemma between a fixed security budget, flexible transaction affordability, and resistance to governance capture under highly liquid utility tokens, Dytallix separates the asset used for consensus weighting from the asset used for execution payment.



This dual-token architecture aligns with established designs (e.g., MakerDAO [11], VeChain [12]), where governance rights and transactional demand are deliberately decoupled, reducing the risk of transient liquidity shocks or flash-loan–based attacks compromising protocol governance.

2.1 DGT: DYTALLIX GOVERNANCE TOKEN

- **Definition:** A fixed-supply asset representing the security weight of the network.
- Supply Constraint: Strictly capped at 1,000,000,000 DGT.
- **Economic Function:** DGT serves as the collateral for Proof-of-Stake (PoS) consensus. It is delegated to validators to increase their probability of leader election via Verifiable Random Function (VRF) sortition.
- **Governance Utility:** DGT is the sole vector for on-chain voting on parameter updates (e.g., fee coefficients, emission bounds).
- **Anti-Ossification Mechanism (Weight Decay):** To prevent permanent plutocratic accumulation and governance apathy, DGT voting power is subject to Activity-Based Decay.
  - **Trigger:** If a staked position fails to vote on eligible proposals (defined as epochs where at least one proposal was active) for > 25,000 eligible epochs, its effective Governance Voting Power decays by a factor of λ_{decay} per epoch.
  - **Reset:** Decay is reset by casting a vote (Yay/Nay/Abstain) or by a "Refresh" transaction.
  - **Attack Mitigation:** To mitigate "Refresh Spam" (cheaply resetting decay without meaningful participation), Refresh transactions are subject to a protocol-level congestion multiplier.
    - **Base Cost:** For Refresh transactions, the base transaction fee F_{tx} is computed using fixed protocol constants $C_{gas}^{refresh}$ and $B_{gas}^{refresh}$.
    - **Multiplier:** During periods where utilization $U > U_{target}$, the fee scales as $F_{refresh} = F_{tx} \times \phi_{cong}$, where $\phi_{cong} \geq 10$, explicitly de-prioritizing maintenance tasks in favor of economic activity.



Note: This decay affects governance weight only. The Consensus Weight (used for leader election and finality) remains based on the raw staked DGT amount to preserve chain security.

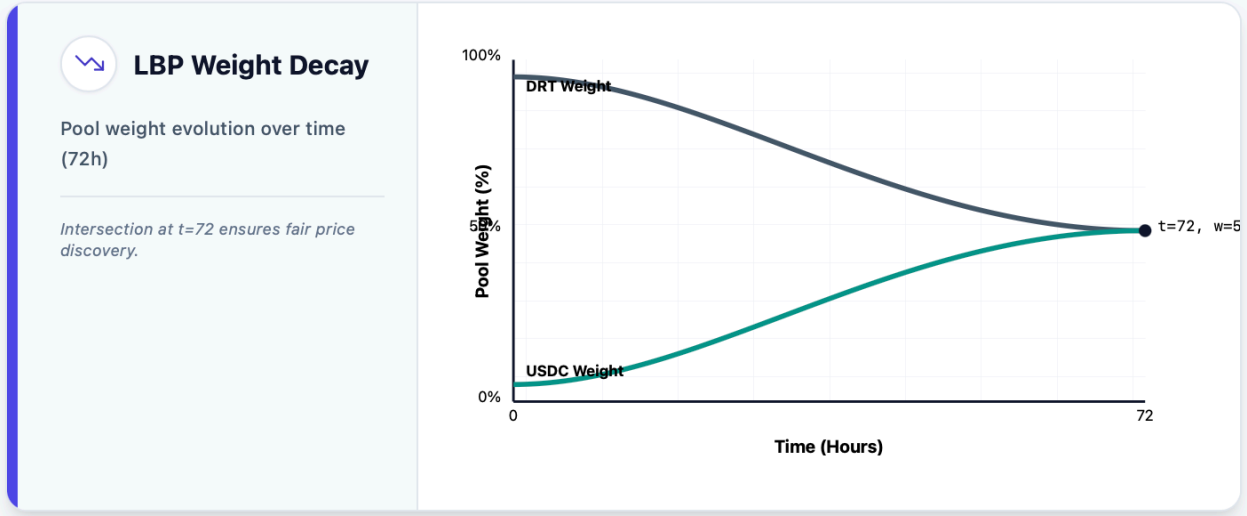
2.2 DRT: THE UTILITY REWARD TOKEN

- **Definition:** An elastic-supply asset serving as the network's unit of account.
- **Supply Dynamics:** The supply is dynamic, governed by the net difference between Minting (via the Emission Controller) and Burning (via the Fee Market).
- **Economic Function:** DRT is used to pay all transaction fees ($C_{gas} + B_{gas}$) and is the currency in which validator rewards are denominated.

DRT is intentionally specified at a higher level of abstraction in this section; its detailed economic behavior is fully defined by the Emission Controller (§3) and the Dimensional Fee Market (§4), rather than by governance mechanics.

2.3 GENESIS LIQUIDITY BOOTSTRAPPING (THE "COLD START" SOLUTION)

To solve the valuation paradox where validators cannot pay OpEx with unpriced tokens at genesis, Dytallix implements a Reverse Liquidity Bootstrapping Pool (LBP) [Module].



- **Mechanism:** A Balancer-style LBP initialized with a ratio of 95% DRT / 5% USDC.
- **Weight Schedule:** The pool weights $w(t)$ shift via a sigmoidal decay function over a fixed window T_{boot} (72 hours), moving from 95/5 to 50/50.
- **Access Policy:** Publicly accessible.
- **Whale Mitigation:** To mitigate late-stage "sniping," a per-address cap is enforced for the final 6 hours of the LBP. Note: While per-address caps are susceptible to Sybil attacks, they act as a partial mitigation by increasing the operational friction and gas costs for attackers attempting to corner the initial supply.
- **Economic Impact:** This creates a continuous price decay curve that counteracts early speculative volatility. It facilitates price discovery by punishing front-running bots and establishing a quantifiable floor price (P_{DRT}) before the first epoch. USDC acts as a temporary transitional bridge asset.

3. Supply Dynamics: The PID Emission Controller

Unlike Bitcoin's static deflationary schedule, Dytallix employs a Discrete PID (Proportional-Integral-Derivative) Controller to govern the issuance of DRT [Core Consensus].

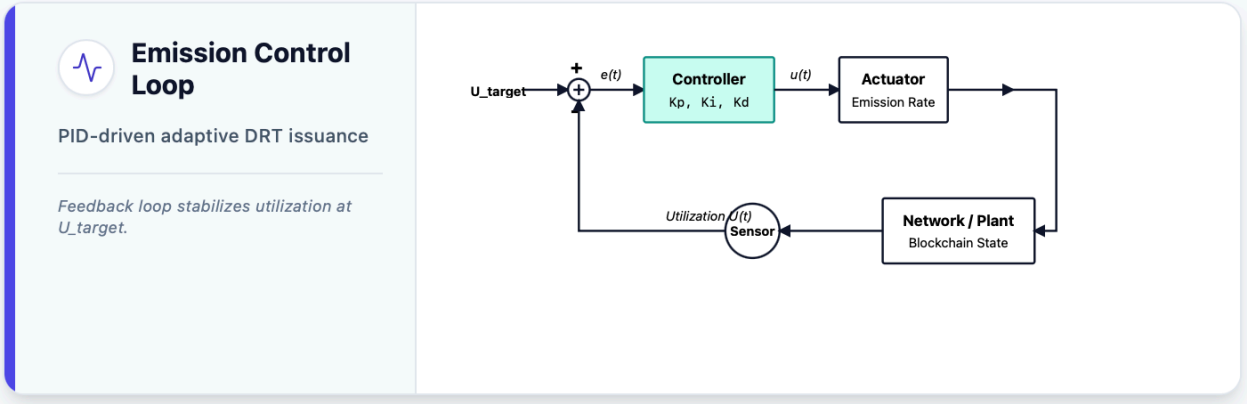
3.1 THE CONTROL LOOP & OPTIMIZATION OBJECTIVE

To address the ambiguity of the optimization goal, the controller explicitly minimizes the following Loss Function J:

$$J = \min \sum_{t} \left((u_{target} - u_t)^2 + \gamma (\Delta E_t)^2 \right)$$

Where the first term minimizes utilization error (ensuring security budget matches demand) and the second term minimizes emission volatility (ensuring validator revenue predictability). The PID gains K_p, K_i, K_d are derived via offline Monte Carlo simulations to minimize J.

These demand curves and gain calibrations serve as effective design assumptions subject to empirical validation in a production environment.



The error term e_t is defined as:

$$e_t = u_{target} - u_t$$

The emission rate for the subsequent epoch, E_{t+1} (Total DRT emitted per Epoch), is calculated using the standard form of a discrete PID controller:

$$E_{t+1} = E_{base} + K_p e_t + K_i \sum_{j=t-W}^{t} e_j + K_d (e_t - e_{t-1})$$

Where:

- **Input u_t:** The arithmetic mean of the per-block bandwidth saturation U_b observed during epoch t. (Note: U_b denotes per-block saturation; u_t denotes the epoch-average of U_b.)
- K_p **(Proportional):** Reacts to immediate demand shocks.
- K_i **(Integral):** Corrects for long-term historical drift over window W= 1008 epochs (approximately 1 week), aligning with the unbonding period.
- K_d **(Derivative):** Dampens oscillation to prevent supply instability.

- **Reflexivity Dampener**: To address single-chain isolation risks, if the external market volatility σ_{ext} (sourced via the Oracle Medianizer's dedicated volatility_index field) exceeds a threshold σ_{max}, the gains are scaled down by $\frac{1}{1+\sigma_{ext}}$.

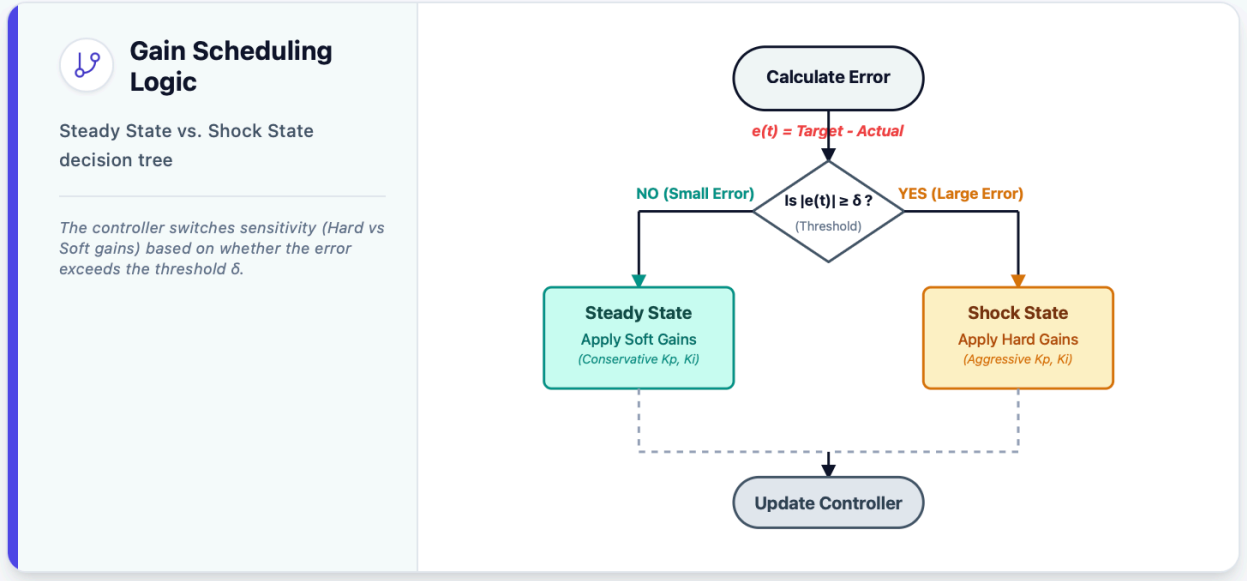
3.2 CONTROLLER STABILITY & GAIN SCHEDULING

To guarantee economic stability across heterogeneous demand regimes, the Emission Controller implements Gain Scheduling constrained by explicit bounded-stability limits.

Regime A (Steady State) When the utilization error magnitude satisfies: $|e(t)| < \delta$, the controller operates in Steady State mode. In this regime, Soft Gains are applied to minimize issuance variance and ensure predictable validator revenue under normal operating conditions.

Regime B (Shock State) When the utilization error magnitude satisfies: $|e(t)| < \delta$, the controller transitions to Shock State mode. In this regime, Hard Gains, specifically an increased proportional gain, are activated to rapidly dampen large demand shocks and restore utilization toward the target. To preserve closed-loop stability, Hard Gains are strictly bounded by $|e(t)| < \delta$, This bound prevents excessive overshoot, oscillation, or instability during abrupt demand transitions.

Anti-Windup Logic To prevent integral windup, where accumulated historical error induces excessive future issuance, the integral term is explicitly bounded via projection onto a fixed admissible interval.



The effective integral term is defined as:

$$I_t = \text{Proj}_{[I_{\min},\, I_{\max}]} \left(\sum_{j=t-W}^{t} e(j) \right)$$

where the projection operator:

$$\text{Proj}_{[I_{\min},\, I_{\max}]}(x) = \min\Big(I_{\max}, \max\big(I_{\min}, x\big)\Big)$$

maps the accumulated error onto the closed interval
[I_{\min}, I_{\max}].

This mechanism ensures that prolonged deviations in utilization cannot force unbounded issuance responses, preserving long-term monetary stability while maintaining responsiveness to sustained demand shifts.

3.3 PLANT MODEL (OPERATIONAL APPROXIMATION)

To justify the PID tuning, we model the "System Plant" (the response of network utilization to emission changes) as a First-Order Lag Process with Demand Elasticity:

$$u_{t+1} \approx \beta u_t + (1-\beta)\, D(E_t, P_b(u_t)) + \epsilon_t$$

For the Monte Carlo simulations, the Demand function is modeled as a Cobb-Douglas utility form $D(E,P) = A E^{\eta} P^{-\mu}$. To ensure physical feasibility, the demand function is clamped to the domain $[0,1]$:

$$D'(E,P) = \min\Big(1,\ \max\big(0,\ A E^{\eta} P^{-\mu}\big)\Big)$$

The stochastic shock term ϵ_t is modeled as a Gaussian distribution $\epsilon_t \sim \mathcal{N}(0,\sigma^2)$ representing exogenous demand volatility.

3.4 SAFETY BOUNDS AND DISTRIBUTION

The calculated rate is clamped by hard governance bounds:

$$E_{final}(t+1) = \min(E_{max}, \max(E_{min}, E_{t+1}))$$

Distribution follows fixed protocol ratios:

- **40% Validators:** Infrastructure compensation.
- **30% Stakers:** Yield for DGT delegation.
- **30% Treasury:** Ecosystem development and PQC research funding.

4. The Dimensional Gas Market

The primary economic vector for PQC networks is bandwidth. An ML-DSA-65 signature (~3.3KB) is orders of magnitude larger than an ECDSA signature. To prevent "Signature Spam" and state bloat, Dytallix implements a Dimensional Cost Function. This approach aligns with multidimensional fee design research (e.g., pricing multiple non-fungible resources separately) to ensure optimal resource allocation.

4.1 THE FEE FORMULA & UTILIZATION METRIC

A transaction fee F_{tx} is the scalar product of its resource consumption vector and the network's dynamic price vector, plus a priority tip:

$$F_{tx} = C_{gas}P_c + B_{gas}P_b(U) + T_{tip}$$

Where:

- C_{gas} (Compute) : The count of WASM instructions (CPU cycles).
- P_c : The base price for compute (relatively static).
- B_{gas} (Bandwidth) : The size of the transaction in bytes (Signature + CallData).
- $P_b(U)$: The dynamic price for bandwidth.
- T_{tip} : User-specified Priority Tip.

Fee Distribution Policy: To align incentives, all bandwidth charges ($B_{gas}P_b$) are burned (removed from supply), creating deflationary pressure during high utilization. Block proposers receive only the Compute Fee ($C_{gas}P_c$) and the Priority Tip (T_{tip}) to compensate for execution resources and inclusion preference.

While dynamic base fee mechanisms reduce unpredictability in fee estimation, their stability depends on update rules and step sizes. Research on EIP-1559 shows chaotic fee behavior is possible under certain conditions [9], emphasizing the need for controlled responsiveness in fee parameters. Empirical studies further indicate that fee mechanisms with base fee burns and tips can improve user experience by smoothing fee volatility and reducing waiting times compared to first-price auctions [10].

Utilization Metric Definition: U_b is rigorously defined as the Bandwidth Saturation Ratio for block b:

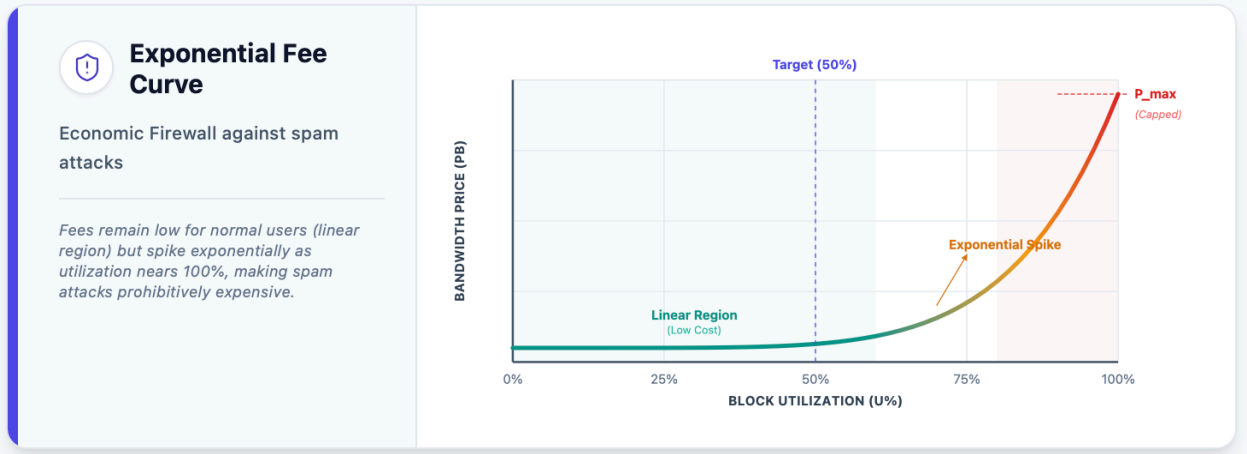
$$U_b = \frac{\sum_{tx \in Block_b} \text{Size}(tx)}{\text{BlockSizeLimit}_{max}}$$

This decouples U from compute load, ensuring the PID controller targets bandwidth specifically.

4.2 EXPONENTIAL SPAM DEFENSE & ALPHA SIGNALING

The bandwidth price P_b scales exponentially relative to utilization U. To prevent a "Fee Cliff" (vertical asymptote), the elasticity coefficient α is dynamically derived via Stake-Weighted Mean Tolerance (SWMT). The function is clamped at P_{max} (e.g., 100x base) to prevent infinite vertical asymptotes.

$$P_b(U) = \min\left(P_{max}, P_{base}e^{\alpha(U-U_{target})}\right)$$



Alpha Signaling Protocol (Cartel Resistance): To address Cartel Risk, the preferred_alpha selection uses a Trimmed Mean (discarding top/bottom 10% of stake weight). Additionally, global α updates are bounded by a maximum change of $\pm$ 5% per epoch to prevent sudden cartel-driven volatility.

- **Signal**: Validators include an 8-byte preferred_alpha value in every block header.
- **Consensus**: The protocol calculates the trimmed stake-weighted mean every epoch.

4.3 VALIDATOR VIABILITY & THE ORACLE MEDIANIZER

PQC networks impose high bandwidth OpEx. Dytallix validators require enterprise-grade uplinks (e.g., 10Gbps symmetric). To prevent validator insolvency, the Emission Controller enforces a Fee Floor **(**F_{min}**)** logic with explicit dimensional consistency:

$$P_{base} \geq \frac{c_{bw}}{p_{drt}}(1+m)$$

Where:

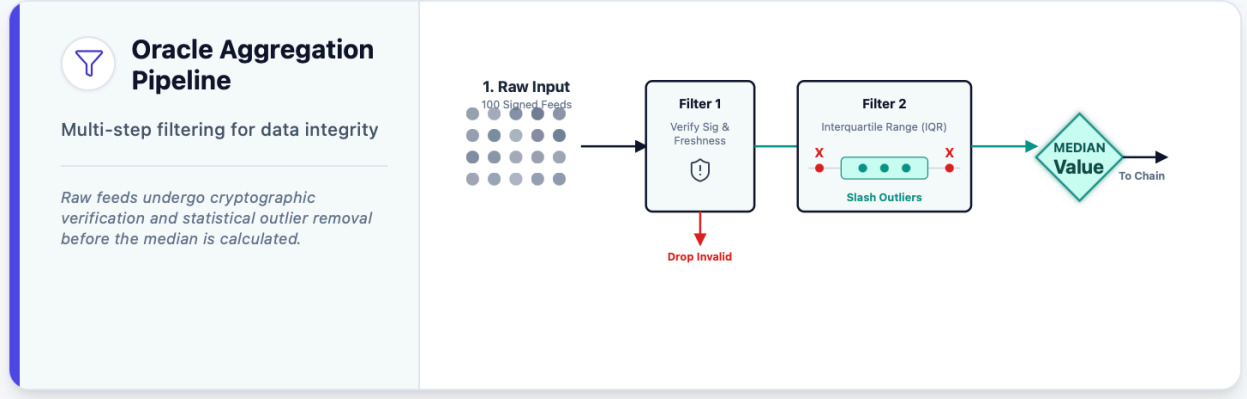
- P_{base} : Base Fee (DRT/byte).
- c_{bw} : Real-world bandwidth cost (USD/byte).
- p_{drt} : Token price (USD/DRT).
- m : Safety margin (e.g., 0.20).

The Oracle Medianizer Solution [Module]: To safely derive p_{drt} and c_{bw} without centralized dependencies and enforce honest reporting, the protocol uses an on-chain medianizer algorithm.

4.3.1 ORACLE ALGORITHM: VALIDATION, AGGREGATION, AND PENALTIES

- **Input**: Each epoch, oracle validators broadcast signed oracle messages via the P2P gossip layer. Block proposers include a batch of these messages in their blocks. The protocol aggregates all unique, valid messages observed across all blocks in the epoch. Uniqueness is keyed by (validator_id, epoch_id). Highest-seq or first-seen wins; duplicates are ignored. Oracle set membership for each epoch is defined as the top-100 validators by effective staked DGT at the epoch boundary (stake snapshot at epoch start).
- **Validation**:
  - **Authentication**: Verify the cryptographic signature against the validator's registered consensus key.

  - **Freshness**: Reject feeds where epoch_id does not match the current epoch.
  - **TWAP**: Verify the reported price is a Time-Weighted Average Price calculated over the previous epoch (100 slots x 2s = 200s).
- **Filtering (Outlier Detection)**:
  - Compute the first quartile ($Q1$), third quartile ($Q3$), and Inter-Quartile Range ($IQR = Q3 - Q1$).
  - **Define the valid range**: $[Q1 - 1.5\,IQR, \quad Q3 + 1.5\,IQR]$.
  - Mark any feed outside this range as an Outlier.
- **Penalties**:
  - Validators submitting Outliers are subject to Progressive Slashing determined by a deterministic schedule: 1st offense: 0.01%, 2nd: 0.05%, 3rd: 0.25%, 4th: 1.0%, 5th+: 5.0%. Offense counts reset after a 30-day rolling window of honest reporting.
  - Validators failing to report for >10% of epochs in a rolling window of $N = 10{,}000$ epochs incur a liveness penalty and Temporary Ejection. Ejection lasts $M = 100$ epochs; during this time, the oracle set is refilled by the next-highest-stake validators. Oracle duty failures do not affect consensus participation (voting/proposing) but do apply oracle-specific penalties.
- **Aggregation**:
  - Discard marked Outliers.
  - Compute the Median of the remaining valid feeds to determine the canonical p_{drt}.
  - Compute the Median of the volatility_index (annualized implied volatility) from non-outlier feeds to drive the PID Reflexivity Dampener.



Note: Median aggregation is used for the final value to ensure robustness against small deviations, while IQR is used specifically for binary outlier classification to enforce slashing.

5. Network Security & Client Feasibility

Beyond gas fees, Dytallix enforces defenses at the P2P networking layer to mitigate attacks targeting the heavier verification time of PQC primitives.

5.1 COMPUTATIONAL ASYMMETRY

The protocol requires that the work required for an attacker to initiate a handshake (W_{solve}) must always exceed the work required for a node to verify it (W_{verify}) by a security factor k:

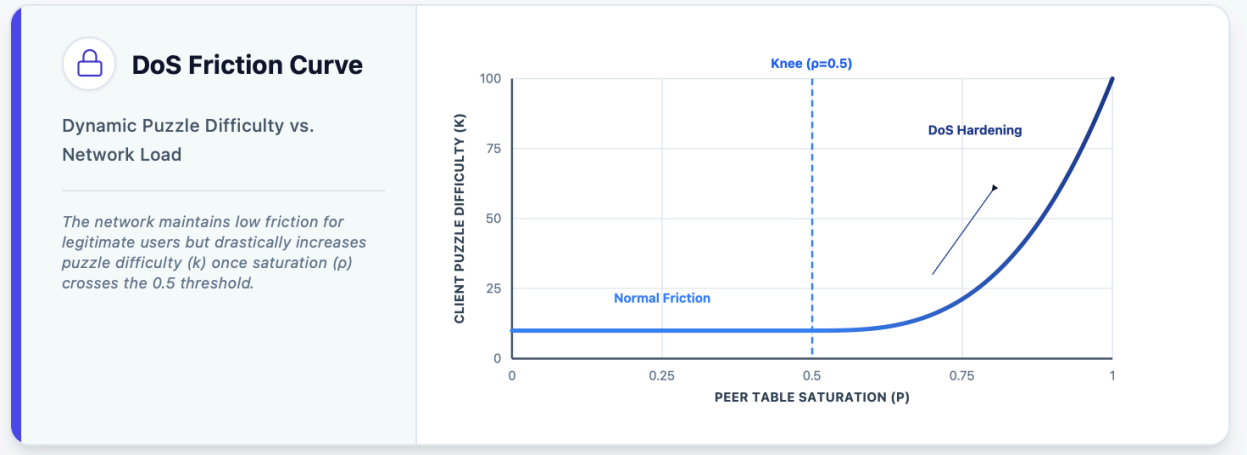
$$W_{solve} \geq k\, W_{verify}$$

5.2 DYNAMIC DOS FRICTION

The security parameter k is dynamic, adjusting based on the peer table saturation $\rho \in [0,1]$.

As the network comes under load ($\rho \geq 0.5$), the difficulty of the client puzzle increases exponentially:

$$k(\rho) = \begin{cases} 100, & \text{if } \rho < 0.5 \text{ (Low Load)} \\ 100e^{5(\rho - 0.5)}, & \text{if } \rho \geq 0.5 \text{ (High Load)} \end{cases}$$



5.3 CLIENT-SIDE FEASIBILITY: THE GATEWAY FEE MARKET

Recognizing that ML-DSA verification burdens low-power IoT/mobile devices, Dytallix introduces Delegated Signing Envelopes (DSE) [Module]. To address Gateway Trust/ Centralization:

- **Mechanism:** Gateways broadcast a fee_rate (DRT per byte) via P2P gossip.
- **Gateway Bonding:** Gateways must post a Service Bond (e.g., 1,000 DRT) to a registry contract.
- **Transparency Log & Fraud Proofs:** Gateways must publish a Signed Transparency Log of received envelopes. If a Gateway wraps a transaction incorrectly or censors a paid payload (proven via receipt vs. log discrepancy), a client can submit a Fraud Proof to slash the Gateway's bond.
- **Redundancy:** Devices utilize Stochastic Redundancy, sending payloads to $k = 3$ distinct Gateways.

6. Incentive Distribution Mechanics

To maintain O(1) complexity for reward distribution, Dytallix utilizes a Global Reward Index rather than iterating through individual staker accounts.

6.1 THE REWARD INDEX ALGORITHM

Let R be the global reward index (cumulative rewards per token). Upon a distribution event of value $R_{stake}(t)$, the index updates as follows:

$$R \leftarrow R + \frac{R_{stake}(t)\, SCALE}{S_{total}}$$

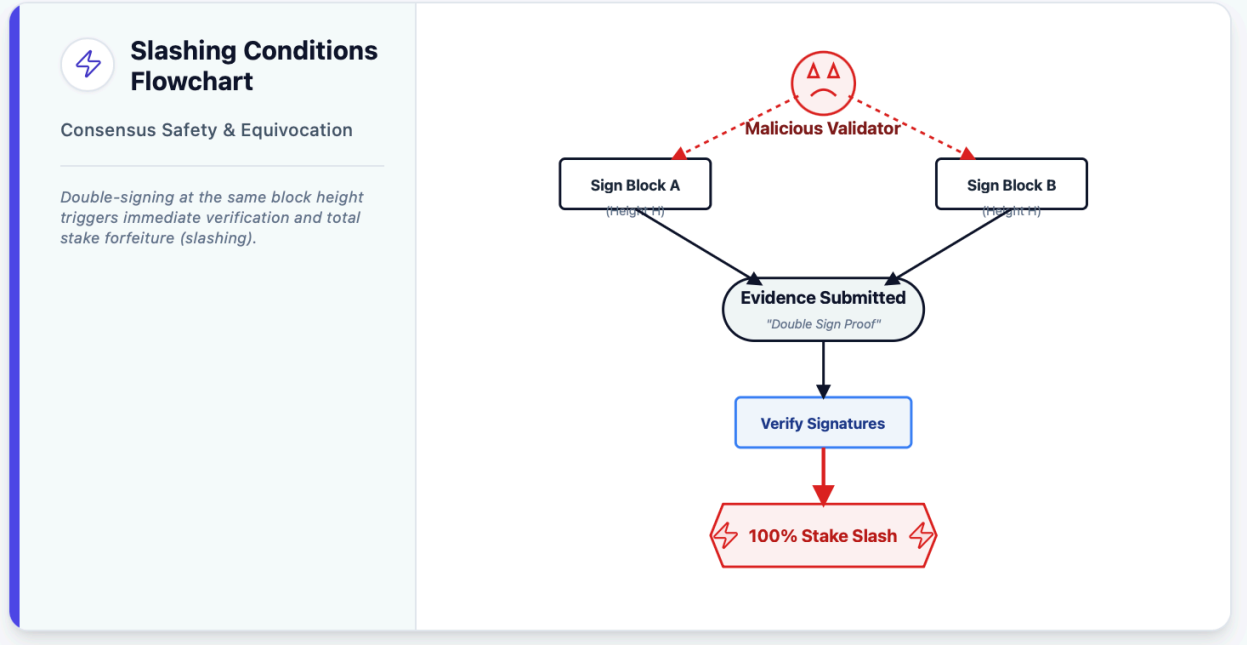
When a user i with stake S_i claims rewards, their payout Δ_i is calculated based on the difference between the current global index and the index at their last interaction ($R_{i,prev}$):

$$\Delta_i = \frac{S_i(R - R_{i,prev})}{SCALE}$$

7. Consensus Safety & Governance Assurance

The integrity of a decentralized system relies not just on its cryptographic hardness, but on the economic cost of subversion and the operational safety of its governance. This section details the mechanisms that ensure consensus finality, protect against governance capture via automated oversight, and secure the bridge for legacy asset migration. By combining proven BFT safety bounds with novel TEE-based optimistic verification, Dytallix creates a defense-in-depth architecture where economic penalties and cryptographic proofs operate in tandem to maintain ledger invariance.

7.1 BFT QUORUM INTERSECTION



Finality requires a supermajority ($> \frac{2}{3}$) of the total stake S. By the Safety Lemma, two conflicting checkpoints cannot both be finalized without an intersection of malicious validators [5]. Because the protocol enforces a 100% Slashing Penalty for equivocation, the economic cost to revert the chain is a proven lower bound of $\frac{1}{3}$ of the total staked market cap (S).

7.2 OPTIMISTIC GOVERNANCE ASSURANCE (CONSUL TEE)

To mitigate the risks of "black box" governance AI, the Consul module [Module] operates as an Optimistic Advisor within a Trusted Execution Environment (TEE).

- **Simulation:** Consul simulates governance proposals off-chain in a TEE (e.g., SGX/TDX) to predict economic impacts.
- **Commit:** It posts a *prediction hash* and ZK-proof of the simulation trace to the chain.
- **Challenge Period:** A 24-hour veto window allows human auditors to challenge the simulation. If a discrepancy is proven (via reproducing the trace), the TEE attestation key is revoked. This restores "Human-in-the-loop" safety.

7.3 INTEROPERABILITY: THE MPC AIRLOCK

Legacy assets migrate via Proof-of-Reserve (PoR**)** utilizing Multi-Party Computation (MPC) [Module]. To address Custody Risk:

- **Key Management:** Legacy asset keys are split into n shards using Shamir's Secret Sharing.
- **Proactive Secret Sharing (PSS):** The protocol enforces periodic **Key Rotation** of the shards themselves without changing the underlying legacy address, ensuring that long-term shard compromise does not reveal the private key.
- **Minting Condition:** PQC-native tokens are minted only upon submission of a ZK-Proof verifying the legacy assets are locked in the MPC address.

8. Security & Economic Assumptions

This section explicitly enumerates the assumptions under which the Dytallix Economic Protocol is secure, stable, and incentive-compatible. These assumptions define the valid operating envelope of the protocol.

8.1 CRYPTOGRAPHIC ASSUMPTIONS

- **Primitive Hardness:** NIST-standardized PQC primitives (ML-DSA, ML-KEM, SLH-DSA) remain unbroken under both classical and known quantum attacks (Shor's Algorithm).
- **Hash Integrity:** Hash functions (BLAKE3, SHAKE256) maintain preimage and collision resistance within stated security margins.
- **Lattice Hardness:** No efficient quantum algorithm exists that solves Module-LWE or Module-SIS at the chosen parameter sets (ML-DSA-65 / ML-KEM-768).

8.2 CONSENSUS & STAKE ASSUMPTIONS

- **Honest Supermajority:** Fewer than $\frac{1}{3}$ of total staked DGT is controlled by Byzantine or economically coordinated adversaries (required for BFT finality).
- **Economic Rationality:** Validators are economically rational in expectation, meaning long-term profit dominates short-term sabotage unless explicitly subsidized by an external state actor.

- **Network Synchrony:** Network synchrony holds within the bounded delay assumptions required for BFT checkpoint finality (messages arrive within 2x slot time).

8.3 ECONOMIC ASSUMPTIONS

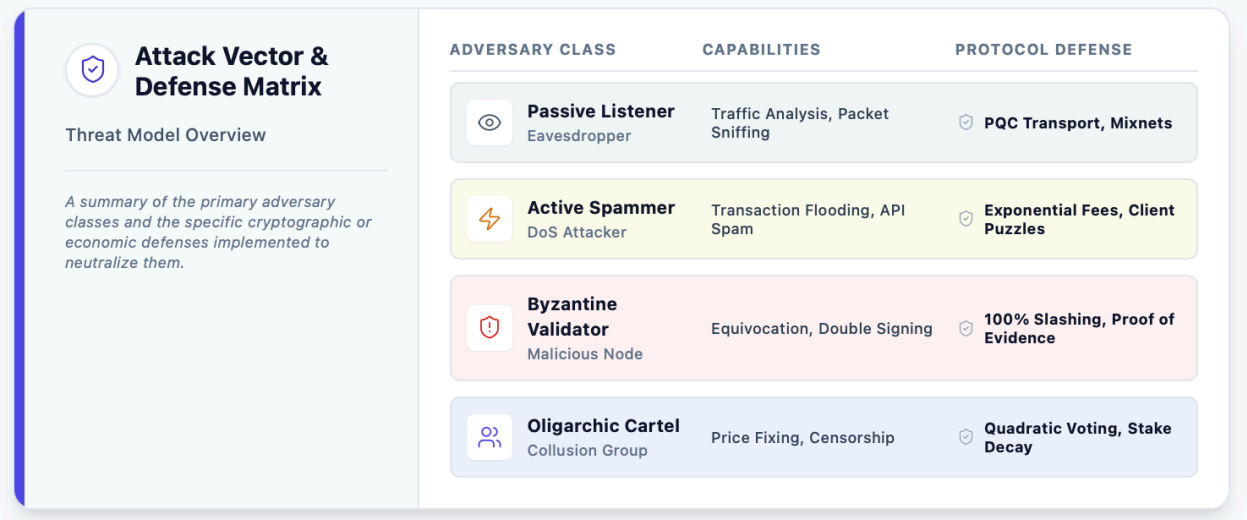
- **Liquidity:** External markets for DRT are sufficiently liquid to price validator rewards without prolonged dislocations (enabled by the Genesis LBP).
- **Heterogeneity:** Bandwidth costs faced by validators are heterogeneous (global distribution) but bounded within an order of magnitude, ensuring fee floors are representative.

8.4 ORACLE ASSUMPTIONS

- **Reporting Honesty:** A majority of top-100 validators report honest price and volatility feeds within statistical tolerance.
- **Cost of Corruption:** Oracle manipulation costs (slashing penalties) exceed expected gains from market manipulation.

9. Formal Threat Model

This section defines the adversarial capabilities Dytallix is engineered to resist and the specific defense posture for each class.



9.1 ADVERSARY CLASSES

9.1.1 EXTERNAL PASSIVE ADVERSARY (THE "LISTENER")

- **Capabilities:** Can observe all network traffic at the ISP/backbone level. Capable of storing all encrypted traffic indefinitely ("Harvest Now, Decrypt Later").
- **Limitations:** Unable to forge PQC signatures or break ML-KEM encryption.
- **Protocol Defense:** All P2P transport is secured via ML-KEM-768 with ephemeral keys, providing Post-Quantum Forward Secrecy.

9.1.2 EXTERNAL ACTIVE ADVERSARY (THE “SPAMMER")

- **Capabilities:** Can spam transactions, attempt DoS attacks on mempools, and exploit fee dynamics. Has no stake or limited stake.

- **Protocol Defense:**
  - **Dimensional Gas:** Decouples expensive bandwidth from cheap compute.
  - **Exponential Fees:** $P_b(U)$ ramps to P_{max} to make spam economically ruinous.
  - **Client Puzzles:** $W_{solve} \geq k\, W_{verify}$ enforces computational friction.

9.1.3 MINORITY BYZANTINE VALIDATORS (< 1/3 STAKE)

- **Capabilities:** Can equivocate (double-sign), delay message propagation, and submit dishonest oracle feeds.
- **Protocol Defense:**
  - **100% Slashing:** Equivocation results in total stake forfeiture.
  - **IQR Aggregation:** Oracle Medianizer filters out statistical outliers.

9.1.4 ECONOMIC CARTEL (< 51% STAKE)

- **Capabilities:** Attempts to bias alpha signaling (spam tolerance), price feeds, or governance votes to maximize rent extraction.
- **Protocol Defense**:
  - **Trimmed Mean:** Alpha signaling discards top/bottom 10% of weight.
  - **Rate Limits:** Parameter updates are bounded (e.g., ±5%).
  - **Governance Decay:** Passive weight decays over time, raising the cost of maintaining control.

9.2 GATEWAY-SPECIFIC THREATS

- **Capabilities:** Censorship or payload dropping by Gateways serving IoT devices. Fee extortion or selective inclusion.
- **Protocol Defense**:
  - **Bonding:** Gateways risk their DRT bond.
  - **Transparency Logs:** Provide cryptographic proof of receipt.
  - **Stochastic Redundancy:** $k = 3$ multipath routing bypasses censoring nodes.

10. Genesis System Configuration

This section enumerates the concrete genesis parameters and their governance-constrained bounds. All parameters are enforced by protocol-level checks at the Consensus and Execution layers.

10.1 CONSENSUS & TIMING

Parameter	Genesis Default	Min Bound	Max Bound	Notes
Slot Duration	2 seconds	1s	5s	High-friction governance update
Epoch Length	100 slots	50	500	Affects decay windows
Finality Threshold	$> \frac{2}{3}$ stake	—	—	Immutable Consensus Rule

10.2 GOVERNANCE & STAKING

Parameter	Default	Min Bound	Max Bound	Notes
DGT Supply	1 Billion	Fixed	Fixed	Hard Cap / Non-Inflationary
Gov Decay Threshold	25,000 epochs	10,000	100,000	Voting Power only (not stake)
Decay Factor (λ_{decay})	0.999	0.99	0.9999	Applied per epoch of inactivity

10.3 EMISSION CONTROLLER (PID)

Parameter	Default	Min Bound	Max Bound	Notes
E_{base}	Governance-set	≥ 0	$\leq E_{max}$	Target DRT / epoch
E_{max}	Governance-set	—	Hard Cap	Inflation Safety Bound
K_p	Tuned	0	K_{p_max}	Regime-dependent gain
K_i	Tuned	0	K_{i_max}	Anti-windup enforced
Integral Window W	1008 epochs	500	5000	Approx. 1 week
Gain Multiplier	2.5x	1x	2.5x	Shock state hard cap

10.4 FEE MARKET

Parameter	Default	Min Bound	Max Bound	Notes
Compute Price (P_c)	Governance-set	≥ 0	—	Relatively static
BW Base Price (P_{base})	Oracle-derived	$\geq F_{min}$	—	Ensures validator viability
BW Price Cap (P_{max})	$100 \times P_{base}$	$10 \times$	$500 \times$	Prevents vertical fee cliffs
Target Util (U_{target})	0.7 (70%)	0.5	0.9	Bandwidth saturation target
Alpha Step Limit	±5%/epoch	1%	10%	Anti-cartel volatility guard

10.5 ORACLE & GATEWAY

Parameter	Default	Min Bound	Max Bound	Notes
Oracle Set Size	100 validators	50	200	Ranked by Stake Weight
Outlier Threshold	$1.5 \times IQR$	$1.0 \times$	$2.0 \times$	Robust Statistics Standard
Gateway Bond	1,000 DRT	100	10,000	Slashing collateral

Redundancy k	3	2	5	Censorship resistance factor

11. Call for Contributors

We actively invite collaboration from the global technical community to harden this specification.

- **Blockchain Engineers:** To optimize the PQC-native P2P layer and Rust-based client implementation.
- **Economists & Game Theorists:** To simulate the PID controller dynamics and stress-test the dimensional fee market against cartel behavior.
- **Mathematicians & Cryptographers:** To audit the lattice-based primitive integrations and formalize security proofs for the consensus safety bounds.
- **Solidity Auditors & Engineers:** To review the smart contract modules (Oracle Medianizer, Consul TEE logic).

Contributors can propose changes via the https://github.com/DytallixHQ or join the Technical Discord at www.dytallix.com.

12. Glossary

- **Airlock Migration:** A custodial deposit-and-reissue process for bringing legacy-chain value into Dytallix.
- **Computational Asymmetry:** A security property where the cost to attack a system is significantly higher than the cost to defend it ($W_{solve} \geq k\, W_{verify}$).
- **Delegated Signing Envelopes (DSE):** A mechanism allowing low-power clients to offload PQC signature generation to Gateway Nodes.
- **Dimensional Gas:** A fee mechanism that prices resources (Compute vs. Bandwidth) independently to account for the specific burdens of PQC signatures.
- **Emission Controller:** A smart contract utilizing PID control theory to adjust token issuance based on network utilization.
- **Gateway Fee Market:** A localized order book where Gateways compete to wrap IoT transactions.
- **Liquidity Bootstrapping Pool (LBP):** A genesis mechanism that shifts token weights over time to discover fair market price.
- **ML-DSA-65:** Module-Lattice Digital Signature Algorithm (FIPS 204), the primary signature scheme for Dytallix.
- **Oracle Medianizer:** An on-chain aggregation mechanism that derives price data from validator-signed feeds.
- **SWMT (Stake-Weighted Mean Tolerance):** A signaling protocol where validators vote on the bandwidth elasticity parameter (α) via block headers.

13. References

1. Dytallix Technical White Paper. January 2026.
2. Dytallix Foundational White Paper. January 2026.
3. Nakamoto, S. (2008). Bitcoin: A Peer-to-Peer Electronic Cash System.
4. Buterin, V., et al. (2020). EIP-1559: Fee Market Change for ETH 1.0 Chain.
5. Gilad, Y., et al. (2017). Algorand: Scaling Byzantine Agreements for Cryptocurrencies.

6. NIST FIPS 204. (2024). Module-Lattice-Based Digital Signature Standard (ML-DSA).
7. NIST FIPS 203. (2024). Module-Lattice-Based Key-Encapsulation Mechanism Standard.
8. Roughgarden, T. (2020). Transaction Fee Mechanism Design for the Ethereum Blockchain: An Economic Analysis of EIP-1559.
9. Leonardos, S., et al. (2021). Dynamical Analysis of the EIP-1559 Fee Market Mechanism.
10. Liu, Y., et al. (2022). Empirical Analysis of EIP-1559: Transaction Fees, Waiting Time, and Consensus Security.
11. MakerDAO. (2017). The Maker Protocol: MakerDAO's Multi-Collateral Dai (MCD) System.
12. VeChain Foundation. (2018). VeChainThor Blockchain Whitepaper.