# FREE: Holder's Guide
## A Utility Token for Deterministic, On-Chain Brokerage

PQSE Research Team

quantaswap@gmail.com

July 2025

**Abstract**

The FREE token is a non-inflationary utility asset designed for use within the PQSE (Post-Quantum Securities Exchange) protocol. Every token is fixed in supply, locked to discrete epochs, and spendable only when unlocked. There is no governance, no rebasing, and no privilege tiers.

FREE enables deterministic trading rebates, allowing holders to access partial or full fee discounts when supplying it in conjunction with trades. Revenue from protocol-level execution fees accrues to holders on a pro-rata basis and is withdrawable via the `speak()` function—subject to a mandatory `speech` payload which enforces proof-of-voice and discourages passive leakage.

All balances, fee mechanics, and distribution flows operate in a 64-bit domain, guaranteeing cross-client compatibility and overflow safety. The contract logic is hardened against third-party custody and tampering, supporting only direct or delegated control. There is no minting function, and all supply is created at genesis. The token's operational state is governed solely by its holders.

This document provides a detailed reference on FREE's role, rebate logic, speech enforcement, and staking architecture, along with user obligations, security constraints, and forward-compatible design choices.

**Keywords:** utility token, protocol rebate, deterministic accounting, speech mechanism, post-quantum, IZRC20, epoch locking

# 1. Design Philosophy

The FREE token was engineered with the principle of irreversible minimalism: 86,400 indivisible units exist, no more and no fewer, issued once at genesis and never minted again. This number corresponds to the number of seconds in a standard 24-hour day, anchoring the system's temporal granularity directly to real-world time.

Every design decision in FREE exists to support the goals of deterministic execution, censorship resistance, and fair economic participation. It is not a general-purpose asset, nor

a speculative vehicle—it is a mechanism for shaping behavior in a non-custodial trading system that enforces best execution and forbids discretionary privilege.

Epochs in FREE are fixed to 1-day intervals. At the beginning of each epoch, any previously locked tokens become automatically unlocked, enabling a clean slate for fee rebate and reward allocation. This design eliminates the need for interactive state updates and ensures predictable, synchronized token behavior across all clients and smart contracts.

There is no mint function. No burn. No pausing. No privileged roles. FREE does not carry governance rights or treasury access. It is a pure bearer instrument that enforces its own rules with contract-level invariants.

Usage of FREE is not optional for traders seeking rebates or protocol dividends. It must be supplied, locked, and spoken for—literally. Passive holding is discouraged; instead, the system rewards explicit participation through a `speak()` mechanism, requiring non-empty intent to extract value.

This is not just a token. It is a contract between equals, enforced by code and paid in full by protocol use.

# 2. Token Mechanics

## 2.1 Fixed Supply and Epoch-Based Locking

FREE has a hard-capped supply of 86,400 tokens. Each token is stored and transacted using 64-bit precision, ensuring compatibility with PQSE's deterministic, overflow-resistant architecture. All balances are subject to epoch-based logic: a token can be locked for one epoch, defined as a 24-hour period (86,400 seconds), after which it is automatically released.

The locking window is enforced contractually. A token may be locked once per epoch, and only by an authorized locker designated by the holder. This restriction ensures that rebates and protocol reward allocations are computed against a stable, committed balance.

## 2.2 Transfer Semantics

FREE is a pure utility token with no built-in burn, mint, or pausing capabilities. Transfers follow strict checks:

- Locked tokens cannot be transferred.
- Batch transfers are allowed only if the aggregate does not exceed $2-1$.
- Approvals (allowances) are 64-bit bounded and non-infinite unless explicitly set as max.

There is no fee on transfer. There is no treasury cut. The contract does not implement any upgrade path or governance hooks.

## 2.3 Rebate Pathway

During trading via PQSE, users may present a balance of FREE up to one full unit (equal to $10^{\text{decimals}}$) in order to receive a proportional fee discount. The discount is computed linearly

up to 100% of the base trading fee (excluding tips), and is applied in both input and output legs of the trade.

This discount is computed off-chain, locked by the trading contract on-chain via the `lock()` interface, and does not consume the token—it simply requires active, visible commitment of balance.

### 2.4 Speaking and Profit Claim

The protocol pays dividends to FREE holders via the `speak()` function. To receive payout, the caller must:

1. Present a non-empty `speech` payload (arbitrary bytes).
2. Possess a non-zero balance of FREE.
3. Have not yet claimed their full share of protocol revenue for the current epoch.

The `want` flag controls whether the caller wishes to receive payment at the time of speech. Even if `want` is false, calling `speak()` still updates the holder's claim base, effectively marking them as current. This enforces active engagement and filters sybil collection attempts.

Protocol revenue is distributed pro-rata over the total FREE supply and is deducted from the global profit pool atomically.

*Speech is not optional—it is the mechanism by which holders prove presence.*

## 3. Protocol Invariants

FREE's core design enforces strict invariants that prevent dilution, overflows, and unauthorized actions. These are not best-effort guidelines—they are hard constraints implemented at the contract level.

### 3.1 Supply Invariance

- The total supply is immutable at 86,400 units.
- There is no mint function. All tokens are minted once, at genesis.
- There is no burn function. Tokens cannot be destroyed.

*Implication:* The supply cannot inflate, deflate, or fork. Economic models that depend on staking or burn pressure must operate externally.

## 3.2 Lock-Time Consistency

- The epoch duration is fixed at 86,400 seconds (1 day).
- Lock state is only meaningful within the current epoch.
- Every lock resets automatically on epoch rollover without user action.

*Implication:* The lock mechanism enforces daily balance declarations. It is not a staking substitute—it is a coordination primitive.

## 3.3 Transfer Boundedness

- All token movements—direct or via allowance—must use unlocked balance.
- Transfer batches are bounded by the 64-bit domain.
- All recipients in batch transfers must be non-zero addresses.

*Implication:* Large holders cannot accidentally brick their balances via overflow. Every operation is auditable and capped.

## 3.4 Locker ACL Integrity

- Only explicitly authorized lockers can lock a holder's tokens.
- Locker authorization is stored per-holder and does not expire.
- Attempts to lock without permission revert with `UnauthorizedLocker`.

*Implication:* Off-chain systems can coordinate lock intents safely, but no unilateral locking is allowed. Each holder is sovereign.

## 3.5 Profit Distribution Monotonicity

- Each holder tracks their last claimed profit baseline per token.
- Claims never exceed the holder's pro-rata share since last update.
- Rounding is always downward; remainder accrues to unclaimed pool.

*Implication:* No holder can claim twice. There is no race condition across calls, even if multiple `speak()` calls occur in the same block.

### 3.6 Speech Enforceability

- All dividend claims require a non-empty speech payload.
- Speech is logged via an indexed event for compliance observability.
- Claims without speech revert.

*Implication:* Participation is provable. FREE is not just a passive income token—it requires an explicit voice.

## 4. Security Model

The FREE token design assumes a zero-trust execution environment. Every balance operation, lock constraint, and dividend allocation is executed with full adversarial safety in mind. There are no soft assumptions about user honesty, UI correctness, or sequencer fairness.

### 4.1 Overflow and Underflow Resistance

All arithmetic is performed using 64-bit unsigned integers where applicable. Internal calculations—particularly fee math—use 256-bit intermediates to avoid rounding errors and overflow bugs.

**Hard Bound:** Any operation that would exceed `2^64 - 1` reverts or is pre-checked.

### 4.2 Lock Enforcement by Epoch

Locks are enforced by comparing the holder's saved `window` value to the current epoch (`block.timestamp / lockTime`). If the window is stale, the lock is treated as expired and reset. This prevents stale locks from bricking a balance indefinitely.

**Invariant:** No lock survives epoch rollover.

### 4.3 Transfer Sanity Constraints

- Transfers revert if the recipient is the zero address.
- Transfers revert if the sender has insufficient unlocked tokens.
- Batch transfers validate array length equality and aggregate sum.
- TransferFrom reuses allowance logic from single transfer paths.

**Design Principle:** There is no partial success. Either the entire transfer executes or the transaction reverts.

### 4.4 Allowance Consistency

The `transferFrom` and `transferFromBatch` functions use a unified internal path for allowance deduction. Allowances of `type(uint64).max` are treated as infinite and are never decremented.

**Guarantee:** No allowance race conditions exist.

### 4.5 Speech as Proof-of-Intent

The dividend claim function `speak()` requires a non-empty `speech` parameter. This ensures every claim is associated with explicit content, enabling:

- Auditable participation records
- Proof of intent from holders
- Alignment with regulator-observable commentary

**Enforcement:** Claims without speech revert immediately.

### 4.6 No Governance, No Backdoor

FREE has no owner role, no upgrade path, no pausing mechanism, and no privileged mint/burn operations. Once deployed, its state machine is immutable.

**Consequence:** There is nothing to compromise. Risk is reduced to user key security and implementation correctness.

## 5. Protocol Economics

The FREE token functions as a deterministic fee-rebate and dividend-sharing instrument within PQSE. It captures a share of protocol revenues and redirects them to holders who explicitly claim them by speaking.

### 5.1 Supply Hard Cap

Exactly 86,400 FREE tokens exist. This figure is chosen to align with a 1-second resolution on a per-day epoch system, allowing natural economic metaphors like "a second of voice per day."

**No inflation. No minting. No rebasing.** The supply is permanently fixed at deployment.

### 5.2 Epoch System

FREE uses a fixed-length epoch of 86,400 seconds (24 hours). Each holder's locked balance resets with every new epoch, enforcing a day-bound staking cadence. This simplifies lock logic, guarantees determinism, and aligns the token with natural time boundaries.

**Epoch formula:**

$$\texttt{epoch} = \left\lfloor \frac{\texttt{block.timestamp}}{86,400} \right\rfloor$$

### 5.3 Fee Rebate Curve

FREE entitles holders to a linear discount on protocol trading fees:

- Holding 0 tokens $\rightarrow$ 0% discount
- Holding 1 full token (i.e., $10^{\text{decimals}}$) $\rightarrow$ 100% discount

Partial holdings interpolate linearly. A user holding 0.25 tokens receives a 25% fee rebate (exclusive of referral tips).

### 5.4 Referral Tips (Optional)

Preparers of transactions may optionally claim a tip—up to 3%—paid by the traders they bring. Tips are not rebated by FREE. The referral path is enforced at the protocol level, not via signature routing.

### 5.5 Dividend Distribution (Speech-Based)

Protocol revenue accrues over time from trading fees. To collect a share, a FREE holder must:

1. Submit a non-empty `speech` string
2. Call `speak()` with the desired token list
3. Opt into collection by passing `want = true`

Holders receive:

```
(profit[token] * holderBalance) / totalSupply
```

The claim resets the user's `bases[holder][token]` tracking pointer.

### 5.6 Optionality and Neutrality

FREE is not required for participation. It merely optimizes the fee path for proactive users. There is no penalty for not holding FREE, only reduced savings.

**FREE exists to reward active engagement, not to extract rent.**

## 6. Rewards and Participation

FREE does not emit inflationary rewards, nor does it promise staking yield in the conventional sense. Instead, the token is rewarded through usage—either directly via protocol dividends or indirectly through fee savings.

### 6.1 Speaking to Earn

The protocol only distributes accrued fee revenue to holders who engage. This is formalized through the `speak()` function:

- **Speech is required:** A non-empty `speech` string must be provided. This can be a note, reference, signature, or commentary.
- **Revenue is opt-in:** Setting `want = true` triggers payment. Leaving it false allows commentary without claim.
- **Transparent record:** All speeches are emitted as events, permanently recorded on-chain.

This design ensures that rewards are not passively streamed, but actively requested. The system pays for voice, not silence.

### 6.2 Pro-Rata and Deterministic

Every distribution is calculated exactly and deterministically:

$$\texttt{share} = \left\lfloor \frac{\texttt{profit[token]} \times \texttt{balanceOf(holder)}}{\texttt{totalSupply}} \right\rfloor$$

No randomness. No gas auctions. The caller either qualifies or they do not.

### 6.3 No Double Dipping

Each holder's last-claimed base is tracked per-token. Attempting to re-speak without new revenue results in a no-op. Even if speech is made, no funds will be released unless profit accrued since the last claim.

### 6.4 Participation Is Costless

There is no minimum lock or burn requirement to participate. Users can earn full rewards for holding a single FREE token and speaking once per epoch.

**The only cost is attention.**

## 7. Governance and Control

FREE does not implement governance.

### 7.1 No Voting Mechanisms

There are no proposals, no DAOs, and no delegates. Token holders do not control protocol upgrades, fee parameters, or execution logic. This is deliberate: FREE is a utility token, not a governance token.

The protocol it interacts with—such as PQSE—is hardcoded and self-contained. Behavior is determined by contract code, not off-chain sentiment or token-majority coercion.

### 7.2 Emergency Halt

The only discretionary power granted to FREE holders is the ability to halt the PQSE exchange in the event of a critical fault.

- **Threshold:** The caller must hold 75% of total FREE supply.
- **Effect:** Halting disables the trading entrypoint on PQSE, rendering it inert but not destructible.
- **Reversibility:** The same threshold can un-halt the system.
- **Non-exclusive:** Anyone with sufficient balance can trigger it; there is no designated multisig or council.

### 7.3 Immutable Parameters

FREE itself is immutable. Its supply, decimal precision, locking window, and associated metadata (e.g. theme) are all fixed at deployment. It has no upgrade path or admin keys.

**There are no upgradable proxies. No backdoors. No kill switches.**

### 7.4 Verified Deployments Only

The token may be verified through the `UtilityTokenDeployer` contract. Any other deployment claiming to be FREE is not recognized by the PQSE protocol and will be rejected by its compatibility checks.

## 8. Future and Philosophy

FREE is not a roadmap. It is a floor.

It provides a minimal, self-enforcing economic interface between builders and holders. That interface is intentionally hard to change—because real guarantees are only meaningful when they resist governance capture, off-chain negotiation, and emergent cartelization.

## 8.1 Value Creation Without Control

FREE cannot enforce what others do with it. That is the point.

Projects may integrate FREE as a fee rebate, a revenue share token, or a speech gating mechanism. They may build tools, marketplaces, games, or fraud-resistant exchanges that reward its holders for participation, commentary, or contribution. No permission is needed.

FREE does not direct capital. It measures conviction.

## 8.2 No Guarantees, Only Constraints

FREE does not promise yields, voting rights, or price appreciation. It guarantees:

- Fixed supply (86,400 units).
- Fixed decimal precision.
- Fixed epoch length (1 day).
- Fixed metadata link (the `theme`).
- Fixed compliance logic (locked balances can't move).

All other behavior is emergent.

## 8.3 Interoperability Over Maximalism

FREE is deliberately unopinionated. It will not attempt to be a Layer-1 token, a store of value, or a community badge. It is simply a 64-bit bounded asset with a well-defined staking window and an on-chain reputation layer via speech emission.

If the system is used, FREE becomes a bottleneck. If the system is abandoned, FREE becomes inert. Its value is contingent, not promised.

## 8.4 Closing Thoughts

You do not need a permission slip to reward people who help.

That is what FREE is for.