$LITKEY Whitepaper

Abstract

Lit Protocol is a decentralized key management network that can be used to facilitate programmable signing, encryption, and compute operations. At the core of the Lit ecosystem lies the **$LITKEY** token, a multi-faceted **work and payment** token that enables the protocol to maintain robust economic security while also functioning as the primary medium of exchange for accessing network services.

This whitepaper provides a comprehensive overview of the $LITKEY token's utility and design principles. It outlines how rewards are distributed to node operators and stakers, how fees are structured for service consumption, and how various parameters—such as staking requirements, price mechanisms, and security measures—collectively sustain a balanced token economy. Furthermore, the document highlights potential evolutionary paths for future token protocol upgrades. After reading this paper, individuals will gain insights into the token's core functionality, the rationale behind its parameters, and the overarching goals of fostering a secure, efficient, and open network.

---

1. Background

1.1 What is Lit Protocol

Lit is a decentralized **key management and compute network** that serves as a private **execution and orchestration layer**, facilitating cryptographic operations across on and off-chain applications, AI agents, and protocols. Lit Protocol solves the generational computer science problem of secret management, introducing a secure, verifiable, and interoperable way to manage secrets for any internet native application or protocol.

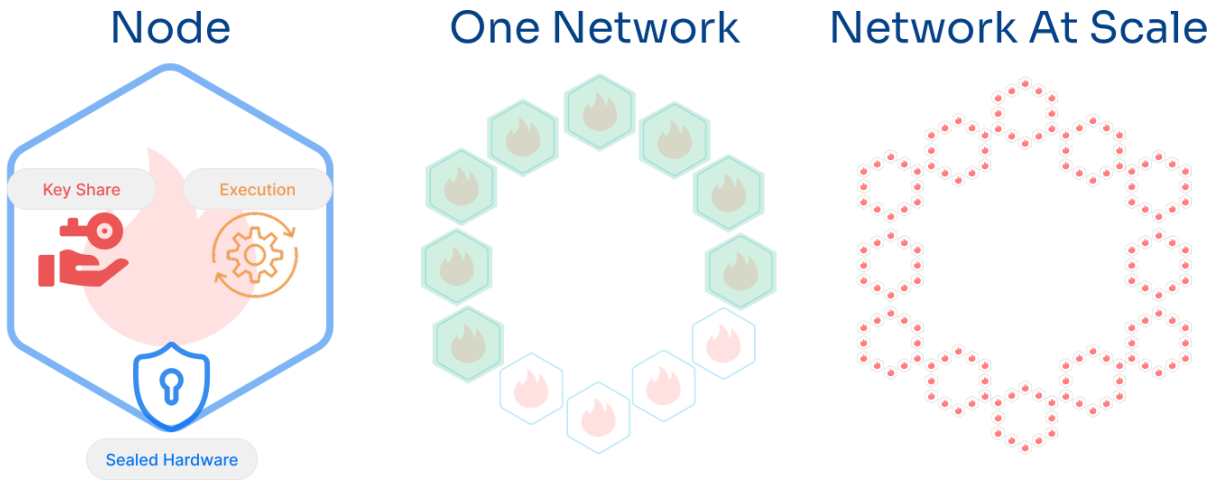
The Lit network provides three primary services: signing, encryption, and private compute. These primitives enable developers to **simplify Web3 onboarding flows**, **transact across previously disconnected ecosystems through chain abstraction, enforce access control rules over private data, facilitate P2P data exchange via open data marketplaces, build autonomous agents that can transact without a human in the loop, verify and consume off-chain data**, and more.

While each blockchain provides a shared state layer for its users, Lit introduces a programmable execution and coordination layer that allows applications to interact with,

authenticate, and modify this state in a decentralized and verifiable manner. Blockchains can be thought of as the base layer for Web3 application development, facilitating transaction settlement and smart contract execution. Lit extends this functionality by providing essential cryptographic infrastructure for **building private and interoperable applications atop public blockchains and other open systems**.

1.2 Lit Protocol Architecture

Lit Node Protocol



The Lit network delivers signing, encryption, and compute services through a decentralized system of independent nodes. Unlike centralized solutions that depend on single-party trust, Lit's core innovation lies in its **distributed cryptographic key management**. By splitting control of private keys across the network and embedding programmable, smart contract-like rules for signing/encryption operations, Lit ensures no single entity holds sole authority. This architecture guarantees verifiable execution of cryptographic rules while eliminating centralized control over sensitive operations.

Each node in the network is responsible for generating and maintaining a share of cryptographic key pairs, leveraging **Distributed Key Generation (DKG) and Threshold Signature Schemes (TSS)**. Under this model, a predefined subset of nodes known as a "threshold" (two-thirds of the network) programmatically collaborate to generate valid cryptographic signatures, decrypt data, or execute secure computations. This threshold-based approach eliminates central points of failure, preventing any single entity from compromising or unilaterally accessing the private key material and other secrets managed by the network.

To further fortify the security of cryptographic operations, all Lit nodes run within **Trusted Execution Environments (TEEs)**. TEEs provide hardware-enforced isolation, ensuring that even if an adversary gains control of a node's infrastructure, **they cannot extract private key**

shares, manipulate computation outputs, or interfere with cryptographic execution. This guarantees that signing, encryption, and computation requests are processed securely, without exposing sensitive key material to node operators.

By combining MPC-TSS with TEE-based execution, Lit establishes a **high-integrity, censorship-resistant framework for performing tamper-proof cryptographic operations**.

Chronicle: the Lit L3

While Lit itself is **not a blockchain**, it relies on **on-chain coordination mechanisms** for managing state and enforcing cryptoeconomic security across the off-chain node network. This is achieved through **Chronicle**, an **Arbitrum Orbit (L3) rollup** that functions as the protocol's **on-chain registry and node coordination layer**.

Chronicle serves several important functions, namely:

1. Registering Keys and Associated Permissions: Each signing key generated by the Lit node network is minted as an ERC-721 token on Chronicle. The permissions associated with these keys are managed via the related smart contracts on-chain.

2. Node Staking and Rewards: Lit nodes must stake $LITKEY tokens on-chain in order to participate in network operations. Staking and rewards distribution take place on Chronicle.

3. Service Payments: Developers who integrate the services provided by the Lit network into their own apps pay for the service via the payment contract deployed on Chronicle.

All Lit node operators also run a replica node for the L3, ensuring Lit's on and off-chain operations remain tightly synchronized.

1.3 The Role of $LITKEY: Establishing Cryptoeconomic Security

While **threshold cryptography and TEEs** provide **technical security guarantees**, the **$LITKEY token** introduces a layer of **cryptoeconomic security** that reinforces **defense in depth**. This token-based mechanism ensures that node operators remain economically incentivized to act according to the Lit node protocol, while also enabling long-term network sustainability.

$LITKEY ensures liveness by requiring node operators to stake tokens in order to participate in the signing, encryption, and compute operations provided by the network. Node operators who violate the conditions set forth by the protocol will have their stake slashed. These conditions are covered in section 3.C. below. By tying network participation to economic value, the protocol ensures that operators have financial risk at stake, reducing the likelihood of

malicious activity. Additionally, token holders who aren't node operators themselves will be able to delegate their $LITKEY stake to a node operator(s) of their choice, curating the set of active node operators and helping distribute cryptographic security across a broader set of participants.

Beyond providing economic security, **$LITKEY ensures the soundness of the Lit network by incentivizing long-term node operations**. Staking rewards are distributed to node operators according to their relative **stake-weight**, calculated based on their total stake and a timelock mechanism that is covered in detail below. There are mechanisms in place to **cap excessive rewards and prevent stake centralization**, covered in depth in section 3.

By integrating **technical security (threshold cryptography and TEEs) with economic security (staking and slashing mechanisms)**, Lit maintains a **multi-layered defense model** that safeguards cryptographic operations against both technical and economic threats. The **$LITKEY** token plays a crucial role in the long-term sustainability of securing the network, ensuring that cryptographic secrets remain decentralized, tamper-resistant, and resilient to adversarial manipulation.

2. Utility

The **$LITKEY** token underpins the entire Lit Protocol ecosystem, serving as a multi-dimensional **work, payment, and governance token**. Together, these dimensions aim to facilitate a self-sustaining token economy in which tokens are staked to secure the network, used as rewards to incentivize operator participation, exchanged to access cryptographic services, and to govern the continued growth and development of the Lit ecosystem. The sections below examine each facet in detail.

2.1 Work Token: Securing and Incentivizing Service Providers

The primary function of $LITKEY is that of a **work token**: It plays a dual role in **enforcing network security** and **compensating participants** for maintaining protocol liveness.

To participate in the Lit network, node operators must stake $LITKEY tokens, committing economic value to signal their reliability and long-term alignment with network security. This staking mechanism ensures that operators have a vested interest in maintaining uptime, executing cryptographic tasks correctly, and adhering to protocol rules.

In addition to securing the network, $LITKEY is also used to compensate node operators who perform signing, encryption, and computation operations by running the core Lit software. The protocol distributes token rewards to operators based on their relative contributions, as covered in section 3.A.

Defense in Depth

Lit is designed with a **defense-in-depth approach**, ensuring that cryptographic operations remain reliable and secure even in the presence of adversarial conditions. This model is built on three distinct security layers, where $LITKEY plays a critical role:

1. **Threshold Cryptography:** No single node holds a complete private key; instead, key shares are distributed across multiple nodes, requiring a threshold of participants to execute a valid cryptographic operation.
2. **Trusted Execution Environments (TEEs):** All cryptographic operations are executed within hardware-enforced isolation, preventing node operators from extracting or tampering with key material.
3. **Cryptoeconomic Security:** By requiring $LITKEY staking, Lit ensures that node operators have direct financial exposure to the integrity of the network. Slashing mechanisms deter misconduct, while staking rewards reinforce honest and consistent participation, creating an incentive-aligned ecosystem.

Through this layered approach, Lit maximizes the cost of attack, making it economically, cryptographically, and physically infeasible for any adversary to compromise the protocol. The $LITKEY work token is fundamental to this model, ensuring that **economic incentives remain aligned with network security, decentralization, and long-term sustainability**.

2.2 Payment Token: Paying for Network Services

Beyond its role as a work token, $LITKEY also functions as a **service payment token**, facilitating both on-chain and off-chain operations with Lit.

As the native gas token for Chronicle, Lit's Arbitrum Orbit-based L3 rollup, $LITKEY is required to make any transactions on-chain, such as when generating new key pairs or staking. Aside from gas, $LITKEY is also to pay for signing, encryption, and compute operations provided by the network. Users and applications consuming Lit's cryptographic services must pay per-transaction fees, ensuring that network resources are allocated efficiently while node operators are fairly compensated. Costs fluctuate based on demand, similar to gas-metering.

An in depth overview of the Lit Protocol payment model will be published ahead of the token and v1 network launch.

2.3 Governance Token: Steering Protocol Development

$LITKEY will also serve as a governance token for the Lit Protocol ecosystem, enabling token holders to direct the ecosystem's evolution through a decentralized, on-chain governance system. Individuals holding $LITKEY will play an important role in selecting network operators,

suggesting core protocol upgrades and feature enhancements, distributing public goods and grants funding, and other related functions. Additionally, token holders influence ecosystem growth by shaping strategies for partnerships, integrations, and network expansion. As the protocol matures, these governance mechanisms will continue to evolve.

At the onset of Lit v1, the Lit Advisory Council will be tasked with overseeing the governance process in tandem with $LITKEY token holders. Documentation on the complete governance process will be released prior to the TGE.

---

3. Implementation

This section outlines the core operational parameters governing the $LITKEY staking and payments. By calibrating node rewards, dynamically adjusting pricing for network services, and enforcing slashing for misconduct, the protocol seeks to sustainably incentivize honest node participation while maintaining robust security guarantees. All parameters described herein are subject to ongoing governance review to ensure alignment with evolving market conditions.

A. Node Rewards: Cost & Stake-Weight Based

The Lit Protocol employs a dual reward structure to compensate node operators:

1. **Cost-Based Component**
   A baseline reward is allocated to each node operator to offset the expenses associated with the required hardware and infrastructure. The baseline reward amount may be adjusted periodically via governance (the Lit Advisory Council), to cover the real-world costs associated with node operations (e.g., server hosting) in their entirety, ensuring operators always break even on the costs associated with running a node and never operate at a net loss. The goal is to preserve a stable pool of node operators even during periods of market volatility, essential for maintaining the shared cryptographic secrets maintained by the network in perpetuity.

   Several configurable parameters go into setting the cost-based component of the Lit node rewards budget, including the price of the $LITKEY token, the costs associated with running a node (denominated in USD), and a target profit margin.

2. **Stake-Weight Component**
   Beyond the cost-based component, a staker's total earnings will be distributed according to their relative **stake-weight**. This stake-weight component is calculated as a function of both the *quantity* of **$LITKEY** tokens staked as well as the *length* of time for which they are locked. This timelock can range from two weeks to two years, depending on the preferences of each individual staker. Longer lock durations yield higher multipliers on rewards, signaling greater commitment and aligning incentives toward long-term network

sustainability. The relative nature of this weighting means that overall rewards depend not only on an individual's stake but also on the staking decisions of other participants.

The formula for calculating stake-weight is as follows:

Stake-weight share of node *i*:

An individual staker's share is simply its own stake-weight divided by the total stake-weight in the system:

$StakeWeight\ (i,t)\ =\ \frac{w(i,t)}{\sum_{j=1}^{(N)} w(j,t)}$ where:

- *StakeWeight (i,t)* = stake-weight share of node *i* at time *t*
- *w(i, t)* = stake-weight of node *i* at time *t*
- *N* = total number of nodes

Cap on individual stake-weight:

To prevent any one node from accruing the majority of stake and network rewards, there is a cap on an individual's share of the total stake-weight:

$StakeWeight\ (i,\ t)\ =\ min\ (\frac{w(i,t)}{\sum w},\ c_{max})$ where:

- $\sum w\ =\ \sum_{j} w(j,t)$ or the total sum of stake-weights across all stakers.
- c_{max}: the maximum allowed stake-weight share per staker. This parameter is updateable, and controlled via governance, which will be overseen by the Lit Advisory Council.

The c_{max} value is dynamic, and calculated using the function $max(5\%,\ 2/N)$ where *N* is the number of active nodes in the operator set.

3. **Calculating the Total Staking Rewards Budget**

The total staking rewards budget is calculated as follows:

$Budget\ (t)\ =\ \$LITKEY_{circ}(t)\ \cdot f(s_r(t),\ \overline{Lock}(t),\ b_{min}, b_{max},\ k,\ p)$ where:

- $Budget(t)$: total staking rewards budget at time *t*.

- $f(\ldots)$: the function for calculating the budget relative to the current circulating supply based on multiple parameters.
- $\$LITKEY_{circ}(t)$: circulating supply of $LITKEY at time *t*.

The additional parameters include:

1. $s_r(t)$: the stake ratio, in other words the percentage of the circulating $LITKEY supply that is staked.
2. $\overline{Lock}(t)$: the average lockup time associated with each stake record.
3. Emission parameters:
    - b_{min}= minimum reward emission rate (relative to supply)
    - b_{max}= maximum reward emission rate (relative to supply)
    - k = kink parameter (caps rewards beyond a certain stake ratio)
    - p = power parameter (controls how fast rewards decrease from b_{max} to b_{min})

The following converts the total rewards budget (above) into the daily rewards distribution formula:

$$Budget(t) \;=\; \$LITKEY_{circ}(t) \cdot \; (1/30) \cdot \overline{Lock}(t)^{p} \left(\frac{b_{max}^{\frac{1}{p}} - b_{min}^{\frac{1}{p}}}{k} \cdot min(k, s_r(t)) \;+\; b_{min}^{\frac{1}{p}} \right)^{p}$$

where:

- The first term, $\frac{1}{30}$, normalizes rewards to a daily (vs. monthly) basis.
- The second term, $\overline{Lock}(t)^{p}$, ensures a higher rewards rate for longer stake periods.
- The third term, $\left(\frac{b_{max}^{\frac{1}{p}} - b_{min}^{\frac{1}{p}}}{k} \cdot min(k, s_r(t)) \;+\; b_{min}^{\frac{1}{p}} \right)^{p}$, adjusts total reward emissions based on the total stake ratio.

Sustainability Targets
The parameters above will be monitored closely by the Lit Advisory Council and adjusted as necessary to preserve a sustainable and balanced token economy. The initial parameters will be set ahead of the TGE.

B. Pricing Model (Demand-Side)

A dynamic pricing formula governs transaction fees on the Lit network. Service consumption—encompassing signing, encryption, and computation—incurs fees denominated

in **$LITKEY**. The formula responds to network usage and capacity, allowing for adjustable minimum fees and surge rates during periods of high demand. These parameters are periodically reviewed and updated by governance to reflect real-time supply-demand conditions, as well as external factors such as technological advancements and market sentiment.

More information on the Lit Protocol pricing model will be provided ahead of the launch of Lit's v1 Mainnet, Naga.

C. Slashing

Slashing has been implemented to ensure that node operators keep their machines online and responsive at all times, preventing any downtime that could disrupt the network. Unlike some other protocols where slashing may also enforce computational 'correctness,' Lit Protocol relies on Trusted Execution Environments (TEEs) and threshold consensus mechanisms to guarantee the accuracy and integrity of operations. As a result, slashing in Lit Protocol is **specifically designed to enforce availability and liveness** rather than correctness.

Slashing Conditions

Unresponsiveness: If a node operator is detected as unresponsive by its peers, it will be kicked from the active node operator set. To safeguard the network's security, an immediate epoch transition is triggered, recalculating the threshold to two-thirds of the remaining active nodes. The kicked node will automatically attempt to rejoin the network in the next epoch, which occurs every hour, providing a built-in opportunity to recover from temporary issues.

To prevent persistently faulty nodes from repeatedly disrupting the network, each node has a **kick counter** that increments each time they're kicked. A node can be kicked up to **5 times** before it is banned from the network. Upon exceeding this limit, the node is banned, and its locked stake is slashed by **5%**. Additionally, if a node goes offline and doesn't rejoin within a 24hr period, they are also banned and slashed. Once banned, the node operator must address the underlying issues causing unresponsiveness. The Lit Advisory Council will then manually review the node's status and unban it only after confirming that it is stable and operational, ensuring that only reliable nodes are readmitted to the active set.

To permit occasional and minor unresponsiveness without severely penalizing operators, a 'decay' mechanism has been implemented. The decay mechanism resets the kick counter at the end of each week, meaning a node can be kicked up to 5 times per decay period (1 week) before being slashed. This serves to strike a balance between enforcing network liveness and giving node operators fair opportunities to rectify temporary issues while protecting the network from chronic instability.

Node operators may be penalized for a variety of reasons, each covered in detail below. Certain behaviors will result in immediate slashing (loss of stake and removal from the node operator

set) while others will result in a warning being issued to the node operator. The node operator will have a pre-defined amount of time to address said warning (known as the “grace period”) before they are slashed. If said warning is addressed in a timely manner, the node will automatically be rejoined to the active node operator set.

Appeals

Slashed funds are sent to a contract administered by the Lit Advisory Council. Slashed funds may be redistributed to node operators and/or token delegators if the slashing event is contested and deemed unjust according to the offense.

Governance Oversight

Outside of integrating slashing outcomes with the Lit governance process to ensure consistent enforcement of rules while maintaining flexibility to address edge cases, the Lit Advisory Council will serve an important role in overseeing the parameters associated with the slashing process itself. This includes configuring the slashing penalty itself, as well as managing the kick counter and decay mechanism.

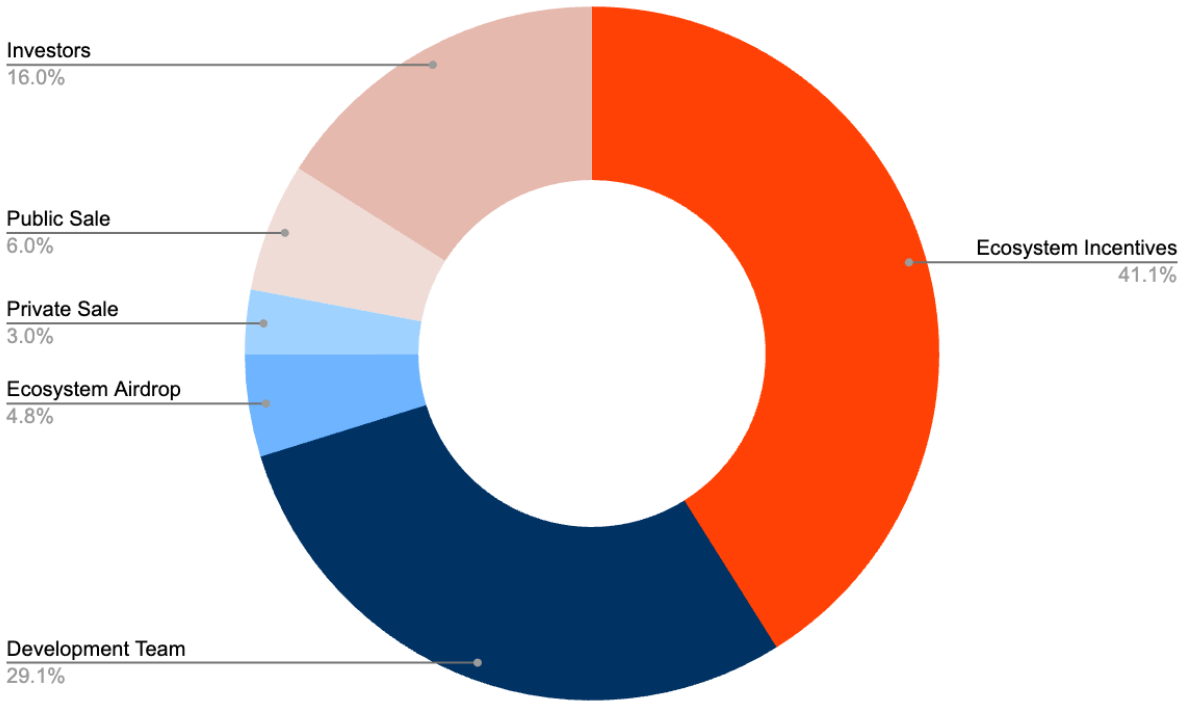
C. Commission

Each node operator is able to set their own rate of commission. This is the node operator’s take on delegated staking rewards.

Through the combination of the above mechanisms, the Lit Protocol token model strives to harmonize operator incentives, price stability, and network security—each facet reinforced by a governance framework that will continue to adapt as the ecosystem matures.

---

4. Token Distribution



- **Investors** – Tokens for Lit investors. All investor tokens are subject to a linear four year vesting schedule with a one year lock following the TGE.
- **Team** – Tokens reserved for the Lit Protocol development team, Workgraph Inc. All team tokens are subject to a four year linear vesting schedule with a one year lock following the TGE.
- **Ecosystem Airdrop** – Tokens allocated to ecosystem builders, testnet node operators, integration partners, and quest participants.
- **Public + Private Sale** – Tokens allocated public sales.
- **Ecosystem Incentives** – Tokens allocated to ecosystem incentives will be used for grant funding, node rewards and incentives, ecosystem growth initiatives, and continued protocol development.

---

5. Roadmap & Milestones

As Lit Protocol continues to evolve, the roadmap reflects both immediate goals and planned long-term enhancements for the $LITKEY token model. Below are two key areas of focus on the horizon:

5.1 Rebates: Incentivizing Network Usage

The introduction of **rebates** is a planned upgrade aimed at **rewarding high-volume users of the Lit network**. While rebates are not currently in place, they will be implemented in the future to incentivize usage of the network from a demand perspective and drive broader adoption of Lit's cryptographic services.

Rebates will function as a retroactive incentive mechanism, where users who generate high transaction volumes—whether through signing, encryption, or private computation requests—receive partial refunds on fees paid to the network. By lowering the effective cost for frequent network participants, rebates will encourage greater throughput, deepen network integration across applications, and establish Lit as a preferred cryptographic infrastructure provider.

The parameters governing rebate eligibility, distribution schedules, and refund tiers will be determined through governance proposals and network monitoring, ensuring that the incentive model remains aligned with sustainable token emissions and long-term economic stability.

5.2 Reserve Nodes & Clonenets: Ensuring Service Continuity and Scalability

To maintain high levels of service availability, Lit will introduce **reserve nodes**—a mechanism for dynamically onboarding additional service providers to prevent disruptions and scale the network over time.

Early-Stage Node Onboarding

In the initial stages, additional node operators will be onboarded on an as-needed basis through governance processes. This approach ensures that the network scales in a controlled manner, balancing the supply of cryptographic service providers with anticipated transaction demand.

However, governance-based node onboarding is not a long-term solution for ensuring network resilience. Over time, a more automated and dynamic mechanism for introducing reserve nodes will be developed to guarantee continuous uptime and seamless network expansion.

Automated Reserve Node Rotation

The long-term vision for reserve nodes is to establish a rotational onboarding system, where pre-qualified nodes remain in reserve status until they are required to replace an inactive, slashed, or offboarded node. This system will ensure that network stability is preserved, even as individual node operators exit or experience downtime.

Reserve nodes will be subject to onboarding requirements and staking commitments, ensuring that only reliable and properly incentivized operators are eligible to transition into active validator

status. This design minimizes disruptions while maintaining strong cryptographic guarantees across signing, encryption, and compute operations.

Scaling via Clonenets & App-Specific Networks

Beyond serving as a redundancy mechanism, reserve nodes may also be leveraged to bootstrap new Lit networks, whether for scaling purposes (clonenets) or for application-specific deployments.

- Scaling via Clonenets: In order to scale the Lit network, any number of parallel "Clonenets" may be deployed. Each associated Clonenet will manage the same underlying root keys, but will have a unique set of node operators.

- App-Specific Networks – "Custom" Lit networks tailored to the needs of DeFi protocols, gaming applications, institutional providers, or other "app-specific" use cases. These networks may have any number of restrictions or requirements associated with them, such as KYC for end users or permissioned node operator sets, depending on the use case itself.

By creating a structured reserve node framework with the flexibility to support both continuity and network expansion, Lit will ensure that its cryptographic services remain highly available, scalable, and adaptable to emerging use cases.
