Tokamak Economics Whitepaper V2

Suhyeon Lee · Donghwan Lee · Yeongju Bak · Kevin Jeong*

*Corresponding author: kevin@tokamak.network

Tokamak Network
December 28, 2025

Contents

Summary

Ethereum was founded to establish a decentralized and censorship-resistant global computer, prioritizing trustlessness and security above all else. However, maintaining this level of decentralization inherently limits transaction throughput on the mainnet. To overcome this scalability constraint while preserving Ethereum's robust security, the industry has adopted Layer 2 rollups as the standard infrastructure. This architectural progression allows execution to occur off-chain, ensuring that the mainnet remains the security anchor for correctness and safety.

As this Layer 2 ecosystem matures, distinct needs for customization and sovereignty are driving the market beyond general-purpose solutions. Developers and enterprises increasingly require dedicated execution environments that offer flexibility and ownership over their infrastructure. This demand is catalyzing the rise of small rollups, which are agile, application-specific networks tailored to unique business requirements rather than sharing a monolithic state. We identify this shift toward modular, customized chains as the next major phase of blockchain utility.

Nevertheless, this fragmentation introduces a critical security crisis. While deploying a custom rollup is technically accessible, establishing a decentralized and reliable verification system remains resource-intensive. Small and independent rollups often struggle to attract a sufficient number of validators and liquidity providers. Consequently, these networks are disproportionately exposed to the *verifier's dilemma*, where the economic incentives for honest monitoring are insufficient, leaving them vulnerable to censorship or operational failure.

Tokamak Network resolves this structural problem by providing a shared verification economics layer. We offer a unified platform where independent small rollups can inherit institutional-grade security without the burden of bootstrapping it alone. At the core is the TON token, serving as the universal asset for security bonds, gas, and governance. Through mechanisms such as the Randomized Attention Test (RAT), we align the incentives of validators to ensure continuous and high-integrity monitoring across the entire network, regardless of the size of an individual rollup.

To guarantee long-term stability, this whitepaper introduces *TON Staking V3*, a performance-driven distribution model. Unlike traditional systems that reward passive capital, V3 allocates protocol seigniorage based on effective economic activity, specifically measured by Bridged TON. This structure ensures that the value of TON grows in tandem with the collective success of the rollup ecosystem, establishing a sustainable economic blueprint for a secure and decentralized future.

1. Verification economics

In this section, we explore the fundamental challenges of blockchain scalability and the necessity of verification economics. We outline the roles of key actors within the Tokamak Network ecosystem and introduce risk mitigation mechanisms that strengthen validator-aligned security and improve the reliability of participant behavior.

1.1. **Blockchains scalability and verification concerns.**

Early general-purpose blockchains attempted to scale by increasing on-chain execution capacity. However, execution throughput, state size, and verification cost tend to grow together. As the chain becomes more heavily used, full nodes must process more transactions per unit time, store a larger global state, and spend more resources to verify new blocks. Over time, this creates an implicit economic filter: only entities that can afford the rising operational cost can remain fully verifying participants.

Rollup-based architectures decouple execution from base-layer consensus[2]. Execution is moved to a separate layer (an L2 rollup) while the L1 blockchain like Ethereum provides data availability and a final arbiter of correctness. In this model, the bottleneck is not how many computations the L1 can perform, but how many state transitions it can verify or accept as economically safe. Rollups extend the total execution capacity of the ecosystem, but they do not eliminate the requirement that at least some participants continuously monitor and verify off-chain activity.

There are two dominant rollup constructions. Optimistic rollups assume that submitted state transitions are valid by default and rely on *fraud proofs* (or called fault proofs): if any party detects an invalid state transition, it can submit a proof that demonstrates the fraud to the L1 [13, 12]. ZK rollups require each batch of state transitions to be accompanied by a succinct cryptographic proof of correctness, known as a validity proof [1]. Both models improve scalability, yet both are constrained by verification: someone must either detect and prove fraud, or produce and verify succinct proofs. In addition, both models are subject to data-availability constraints that must ultimately be resolved on the L1.

Verification in such systems is not free. Monitoring rollup activity requires computational resources and capital at risk. Submitting fraud proofs or producing validity proofs incurs gas costs and opportunity costs. On the other hand, the economic damage from a successful attack (for example, inclusion of a fraudulent batch or failure to respond to an invalid state transition) can be much larger than the individual cost that a single verifier faces. Without explicit incentives, rational agents have little reason to bear the full cost of verification, and verification becomes underprovided[9].

The core design problem is therefore economic. The protocol must ensure that the expected reward for honest verification, and the expected penalty for dishonest or negligent behavior,

are large enough that rational agents prefer to verify[11, 8]. This is what we call *verification economics*. A verification-economics layer is responsible for:

- assigning well-defined roles and responsibilities to actors such as sequencers and validators,
- allocating rewards to those who perform verification and monitoring work, and
- imposing penalties on those who introduce or tolerate incorrect state transitions.

In the Tokamak Network ecosystem, the TON token is the asset that backs this verification-economics layer. TON is staked by ecosystem actors to provide an economic bond that can be penalized if they misbehave or fail to fulfill their verification duties. Rewards that originate from protocol-level seigniorage are distributed to these stakers when they act honestly. The verification layer is designed to be *proof-system agnostic*: while the present exposition focuses on optimistic rollups and fraud proofs, the same economic framework can be applied to validity rollups. In particular, the security condition that adversarial behavior must be economically disincentivized (i.e., expected loss exceeds expected gain) applies whether invalid behavior is detected ex post via fraud proofs or ruled out ex ante via cryptographic validity.

1.2. **Tokamak Network (TON) rollup ecosystem.** Tokamak Network is a multi–rollup framework on Ethereum that uses TON as a common economic security and governance asset. Each Tokamak L2 rollup (hereafter simply 'L2') is operated by a set of actors whose incentives are coupled through TON staking and reward mechanisms. Figure 1 illustrates the high-level architecture and the structural relationships between these key components within the Tokamak Network ecosystem. The ecosystem consists of the following components.

Sequencers. Sequencers are responsible for the overall validity and liveness of the L2 chain. Their core duties include collecting transactions, ordering them, and executing them off-chain. Furthermore, in the network's current state, the Sequencer also assumes the role of the Proposer, periodically posting batched transaction data and state commitments to Ethereum. This integrated model ensures operational efficiency, though the protocol is designed to recognize the logical distinction between ordering (sequencing) and L1 submission (state proposing) for future decentralization.

To participate as a sequencer for a particular L2, a rollup operator must stake TON. The size and conditions of this stake are specified at the protocol level and can be refined through governance. A sequencer earns revenue from L2 transaction fees and from protocol-level rewards that are allocated to its L2, but it is also subject to penalties: if the sequencer attempts to

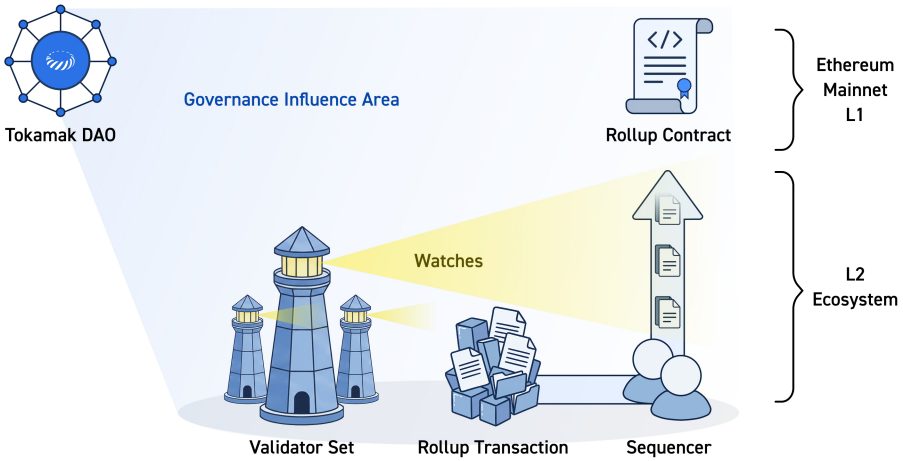

FIGURE 1. Tokamak Network Ecosystem Overview

introduce invalid state transitions, censors transactions in violation of protocol rules, or fails to meet availability and liveness requirements, its stake can be slashed.

Validators. Validation is permissionless: any actor may monitor L2 activity and check that sequencers' state transitions are correct. In an optimistic rollup setting, validators can submit fraud proofs to the L1 when they detect invalid transitions.

Validators may optionally register as *staked validators* by staking TON as economic collateral to provide continuous verification. Staked validators are eligible for protocol-level incentives tied to the overall performance of the L2 ecosystem and may earn fees and bounties associated with successful fraud proofs or challenge outcomes. If a staked validator fails to perform required verification tasks or submits false claims, the protocol can slash its stake. The precise staking and slashing rules are described in later sections.

Tokamak Network will support a *shared validator set* across multiple L2s. A validator stakes TON once and can then participate in the verification of several L2s according to protocol-defined rules. This structure allows smaller and early-stage L2s, which may not have sufficient fees or stake to sustain dedicated validator sets, to inherit meaningful economic security from the global TON staking pool rather than having to bootstrap their own isolated validator sets. It also enables cross-rollup diversification for validators and improves overall capital efficiency of the verification layer.

TON DAO. The TON DAO (Decentralized Autonomous Organization) is the governance body responsible for setting and updating protocol parameters, including those related to verification economics. The DAO authorizes treasury allocations under its governance process. The treasury may hold TON and other assets. A portion of newly issued tokens and protocol revenues is sent to the DAO treasury, which can be used to support public goods, bootstrap new L2s, or adjust the incentive structure when necessary. The DAO can, for example, adjust challenge windows, slashing ratios, minimum stake requirements, or the relative weight of rewards allocated to sequencers and validators. In this way, the DAO acts as a meta-layer that maintains the long-term sustainability of the verification-economics framework.

High-level TON flows. Across these components, the TON token plays several interconnected roles:

- as staked collateral for sequencers and validators, which backs the economic security of each L2,
- as a fee asset for L2 transactions, whose collection and distribution rules are governed at the protocol and DAO levels, and
- as the unit in which protocol-level seigniorage and rewards are denominated and allocated to L2 participants.

Subsequent sections describe in detail how staking and slashing define L2 security, how gas fees are collected and distributed, and how seigniorage is generated and allocated across the L2 ecosystem. In the remainder of this section we focus on specific mechanisms that mitigate core risks in optimistic rollups and shape the economic incentives of verifiers.

1.3. **Risk mitigation mechanisms.** Optimistic rollups introduce a specific family of risks. Sequencers may attempt to post invalid state transitions or censor transactions. Validators may fail to monitor the system or to respond to fraud in a timely manner. Users and liquidity providers face withdrawal delays and bear the risk that the system does not respond correctly to invalid states during the challenge period.

While optimistic rollups rely on the straightforward assumption that there is at least one honest validator, the verifier's dilemma [9] still arises in blockchain systems, and related failures have been observed in practice [5]. Tokamak Network proposes two complementary mechanisms at the economic layer to address these incentive risks: the Randomized Attention Test (RAT), which incentivizes continuous verification effort by validators, and Fast Withdrawal, which allows users to exit L2s more quickly while tying liquidity provision to the security guaranteed by staked TON.

1.3.1. *RAT.* In an optimistic rollup, honest validators face a natural trade-off between the cost of continuously monitoring L2 outputs and the relatively low per-batch probability that any given state transition is fraudulent. Absent additional incentives, it can be individually rational for validators to reduce their level of attention and free-ride on the verification efforts of others, which undermines the security that staked TON is intended to provide. To deal with this, an attention test was proposed as a protocol-level mechanism that occasionally and unpredictably forces this latent verification decision to the surface by assigning explicit verification tasks backed by stake, so that neglecting verification becomes a dominated strategy.

RAT instantiates this idea by randomly selecting subsets of validators at unpredictable times and requiring them to verify specific L2 batches within a given time window, using their staked TON as economic backing. Selected validators must check the batch and submit an attestation to its correctness. Those that respond promptly with honest attestations receive a validator fee, while those that fail to respond or are proven dishonest are subject to slashing. RAT is designed using game-theoretic principles so that the expected cost of reduced attention is higher than any short-term savings from skipping verification, aligning validators' best response with sustained monitoring of L2 outputs.

1.3.2. *Fast Withdrawal.* While the RAT focuses on aligning validators' incentives for continuous monitoring, a complementary approach to mitigating risk operates through withdrawal latency and liquidity. In both optimistic rollups and zk-rollups, users typically face a non-trivial delay between initiating a withdrawal and receiving L1 assets, whether due to a challenge period or proof-generation and finalization constraints. Although advances in rollup design and proving systems are likely to reduce withdrawal delays over time, it is unlikely that such delays disappear entirely. As long as some latency remains, there is economic room for specialized liquidity providers who front assets to exiting users in exchange for a fee, and then redeem the underlying withdrawals once they are finalized on L1. Fast Withdrawal addresses this latency by allowing users to exit a rollup and receive L1 assets (including TON and other tokenized assets) immediately, by borrowing liquidity from dedicated providers.

Fast Withdrawal providers effectively act as an additional layer of economically motivated verifiers. They stake their own assets and assess the current L2 state and withdrawal validity before fronting liquidity, then continue monitoring for signs of misbehavior while their capital remains at risk. The same economic security that backs L2 state, including staked TON and slashing rules, can penalize misbehaving sequencers and validators and compensate affected providers if fraud is later detected and the rollup state is reverted, thereby reinforcing the verification economics established by RAT.

2. Utilities of TON

In this section, we define the three primary utilities of the TON token within the L2 ecosystem: security, gas, and governance. We detail how each utility connects the token's value to the network's operational integrity and growth.

2.1. **L2 security.**

TON strengthens L2 security through a multi-tiered structure rather than a single mechanism. This tiered security model is designed so that sequencers, validators, and challengers function independently yet complement one another, with TON-based economic penalties (slashing) enforcing correct behavior at every stage.

The first tier (Tier 1) is the public challenge (fraud-proof) mechanism. If a sequencer submits an invalid state transition, anyone can submit a fraud proof to dispute it. If the sequencer's state transition is proven to be fraudulent during the challenge process, it is subject to slashing. This serves as the fundamental safeguard ensuring that incorrect states will not finalize on Ethereum L1. However, since public challenges do not define explicit verification roles, it remains uncertain who will actually perform verification.

The second tier (Tier 2) consists of dedicated validators with explicit verification responsibilities. Validators monitor and verify sequencer state transitions and can immediately raise disputes when they detect invalid states. However, validators also face the verifier's dilemma, as the trade-off between verification cost and low fraud probability creates an incentive to reduce attention and free-ride on other validators.

The third tier (Tier 3) is RAT, introduced in Section 1.3. RAT addresses this incentive problem through probabilistic auditing: validators are randomly selected at unpredictable times and required to verify specific L2 batches and submit attestations within a given time window. Because selection is unpredictable, validators cannot anticipate when they will be tested, making consistent monitoring the dominant strategy. Validators that fail to respond or are proven dishonest are subject to slashing, ensuring that the expected cost of skipping verification exceeds any short-term savings.

Through this multi-tiered structure, both sequencers and validators are economically incentivized to behave honestly. Since slashing at each tier is applied to TON-denominated collateral, L2 security is anchored to the economic foundation of the TON ecosystem.

2.1.1. *Economic Security for Sequencers.*

The economic security mechanisms applicable to sequencers correspond to Tiers 1 and 2 of the three-tiered model. All collateral and slashing are denominated and executed in TON.

Multi-Challenger Fraud Proof. In single-winner challenge systems, only the first valid challenger receives a reward. This creates a problem: if a malicious L1 proposer/builder controls transaction ordering between challenges, honest challengers may be entirely excluded and lose their verification costs. Tokamak Network instead adopts a multi-winner approach, where all valid fraud proofs submitted within the dispute period are recognized and rewarded [7]. This reduces the risk that honest challengers are excluded due to ordering manipulation, regardless of the presence of colluding parties.

Sequencer Deposits. The protocol requires each sequencer to maintain a collateral bond ($D_{\text{sequencer}}$) representing their commitment to the network. Let $C_{\max}$ denote the estimated worst-case on-chain cost of executing a single fraud proof. Since Tokamak Network supports multiple independent challengers submitting fraud proofs concurrently, the bond must cover all challengers' verification costs plus an additional reward pool. Let $H_{\max}$ denote the maximum number of concurrent challengers and $\Delta_{sequencer}$ the additional reward provided by a sequencer. The collateral bond is expressed as:

$$D_{\text{sequencer}} = H_{\max} \cdot C_{\max} + \Delta_{sequencer} \tag{1}$$

Sequencer Slashing. When a fraud proof succeeds, whether submitted by a challenger or validator, the entire bond ($D_{\text{sequencer}}$) is slashed. If n challengers win the challenge (where $n \leq H_{\max}$), each successful challenger receives:

$$R_{\text{challenger}} = C_{\max} + \frac{\Delta_{sequencer}}{n} \tag{2}$$

The remainder is transferred to the protocol treasury. This is intended to provide rewards that can exceed verification costs. A slashed sequencer is suspended from sequencing according to protocol rules. To resume operation, the sequencer must restore the bond within the re-bond period; failure to do so results in permanent removal from the active sequencer set. However, if the system has multi-sequencer enabled, other sequencers can continue L2 operation during this period.

Validator Deposits. Each validator is required to maintain a collateral deposit $D_{\text{validator}}$ that serves as the economic guarantee of its attentiveness. According to recent research by Tokamak Network [6], this can be analyzed from a game-theoretic perspective: each validator faces a binary strategic choice in every epoch, either remain attentive (online) or become inattentive (offline). Let c_m denote the per-epoch cost of maintaining attentiveness. Staying attentive incurs c_m but avoids penalties. Going offline saves this cost but risks being selected by RAT and penalized. Let π_a denote the system-wide probability that RAT triggers an attention test in a given epoch, and let N be the number of validators. When RAT triggers, one validator is selected uniformly at random, so each validator faces a selection probability of $\frac{\pi_a}{N}$. For

attentiveness to be the dominant strategy, the expected penalty from being offline must exceed the cost savings. Let C_{off} denote the slashing penalty for failing an attention test. The RAT equilibrium condition under the model ensuring that online behavior strictly dominates offline behavior is given by

$$c_m \;\leq\; \frac{\pi_a}{N} \cdot C_{\text{off}}. \tag{3}$$

This condition implies that the validator's expected penalty from being offline, $\frac{\pi_a}{N} \cdot C_{\text{off}}$, must exceed the operating cost c_m. Accordingly, C_{off} must satisfy

$$C_{\text{off}} \;\geq\; \frac{c_m N}{\pi_a}. \tag{4}$$

Letting $\Delta_{\text{validator}}$ denote an additional buffer contributed by the validator, the deposit is expressed as:

$$D_{\text{validator}} = C_{\text{off}} + \Delta_{\text{validator}}. \tag{5}$$

This structure ensures that even after a slashing event, the validator retains sufficient collateral ($\Delta_{\text{validator}}$) to continue operating without immediate removal.

Validator Slashing. Slashing for validators is applied solely in the context of RAT. When an attention test is triggered with probability π_a, the selected validator must respond within the required time window. Failure to do so triggers a slashing event in which a penalty C_{off} is deducted from the validator's deposit. If the remaining deposit falls below the minimum threshold $D_{\min}$, the validator must replenish it within a specified period; otherwise, the validator is removed from the active validator set. The mechanism is designed so that, under the chosen parameters, attentiveness is each validator's rational strategy.

2.2. **L2 Gas.** TON functions as the native gas token consumed for transaction execution on L2. Users pay TON for all activities on L2, including contract calls, data processing, and asset transfers, creating an ongoing, utility-driven source of demand for TON. As transaction volume on L2 increases, the amount of TON consumed also rises, meaning the gas utility of TON is closely tied to the scalability and throughput of L2.

For TON to serve as a gas token, an L2 must secure sufficient TON liquidity and establish TON-based payment pathways. This structure positions TON not merely as a transaction fee token but as a foundational asset for economic activity occurring on L2. The more L2 services are designed around TON, the more TON becomes the standard asset across the entire ecosystem.

L2s must post data to Ethereum L1 during operation, and the associated L1 security costs must be paid in ETH. For TON to remain a sustainable gas token, the aggregate demand for TON within L2 must exceed the ETH costs required for L1 settlement. By expanding TON utilities such as gas payments, bridging, fast withdrawals, and dApp services, L2s can generate

sufficient TON-denominated value to offset L1 security expenses. For example, fast withdrawal services create a structure where liquidity providers deposit TON and receive withdrawal gas fees in TON, thereby strengthening both TON utility and liquidity simultaneously.

The use of TON for transaction execution and asset bridging on L2 promotes a cyclical pattern of utilization. As TON usage increases on L2, the volume of bridged TON also expands, which in turn supports the emergence of diverse dApps and services built around TON. When this reinforcing loop emerges (L2 growth $\rightarrow$ increased TON transactions $\rightarrow$ increased bridged TON $\rightarrow$ expansion of TON-based services), TON becomes a common and self-sustaining value-transfer asset within a multi-rollup environment.

2.3. **DAO Governance as a Utility of TON.** TON functions as the sole governance asset within Tokamak Network, enabling a decentralized and economically grounded decision-making framework. Governance authority is not assigned arbitrarily; it is earned through TON staking and expressed through the DAO's on-chain committee mechanism.

Tokamak DAO was designed from the outset with a multi-rollup environment in mind, enabling L2 operators and sequencers to participate directly in governance. The Tokamak Rollup Hub SDK includes a pre-deployed contract for DAO participation. This allows L2 operators to join the DAO simply by staking a minimum amount of TON without developing a separate contract, naturally linking L2 identity and governance participation through TON.

Governance influence is determined by the amount of staked TON. Participants with larger stakes have greater say in protocol decisions. This structure ensures that governance power reflects measurable economic commitment and aligns participant incentives with the long-term health of the network.

Through this structure, TON becomes integrated with the lifecycle of L2 development. L2 networks with meaningful economic activity gain stronger incentives to accumulate TON. This secures their operational presence and grants governance authority over protocol parameters and reward distribution. By making TON the exclusive instrument for governance participation and agenda approval, Tokamak Network grounds governance in transparent, on-chain economic metrics.

3. Seigniorage

In this section, we present the mechanism of seigniorage generation and its distribution through TON Staking V3. We analyze the inflation schedule and the mathematical models ensuring the sustainable growth of L2 networks.

3.1. **Sustainable Growth of Layer 2.** TON seigniorage incentivizes sequencers to grow their L2 networks. Since seigniorage revenue is proportional to Bridged TON, sequencers are motivated to attract depositors and increase total deposits. However, deposit growth alone does not guarantee sustainability. If deposits are concentrated among a few large participants, a single withdrawal can destabilize seigniorage revenue. Sequencers will therefore work to diversify their depositor base by attracting various dApps and liquidity providers.

As the depositor and user base grows and diversifies, sequencers can secure additional revenue sources beyond seigniorage: flexible fee policies, high-value applications, and other cash flows within the L2 ecosystem. This TON revenue is used to cover Ethereum L1 security costs, which must be paid in ETH. Even if sequencers sell TON to pay L1 fees, TON demand generated within the L2 ecosystem (such as utility fees) may offset this and help reduce net selling pressure under certain conditions. Seigniorage thus drives deposit growth while a diversified user base improves resilience, and together they form a more sustainable economic structure.

3.2. **Seigniorage Generation.** TON Seigniorage is generated at a fixed rate per block, which determines the inflation dynamics of the network. Let S_0 denote the initial supply and S_{annual} the annual seigniorage. The total supply at year t is $S(t) = S_0 + S_{annual} \cdot t$. The inflation rate at year t is defined as:

$$r(t) = \frac{S_{annual}}{S(t)} = \frac{S_{annual}}{S_0 + S_{annual} \cdot t} \tag{6}$$

As a baseline rule, the protocol issues 3.92 TON per Ethereum block interval. Before the Merge, blocks were produced approximately every 13 seconds, yielding an annual seigniorage of about 9,509,317 TON. Since the completion of the Merge on September 15, 2022 [3], Ethereum's block time has been fixed at 12 seconds, resulting in an annual seigniorage of approximately 10,301,760 TON. Given $S_0 = 50{,}000{,}000$ TON and $S_{annual} \approx 9{,}509{,}317$ TON (pre-Merge), the initial inflation rate is approximately 19.0%. Over time, the inflation rate decreases as total supply grows, reaching about 7.3% after ten years and approximately 1.9% after fifty years. The discontinuity by the red dotted line in Figure 2 reflects the Merge transition point.

3.3. **Seigniorage Distribution: TON Staking V3.** Seigniorage distribution refers to the allocation of newly issued TON to participants. In TON Staking V3, the distribution amount is determined based on each L2's Bridged TON. L1 staking does not determine the distribution

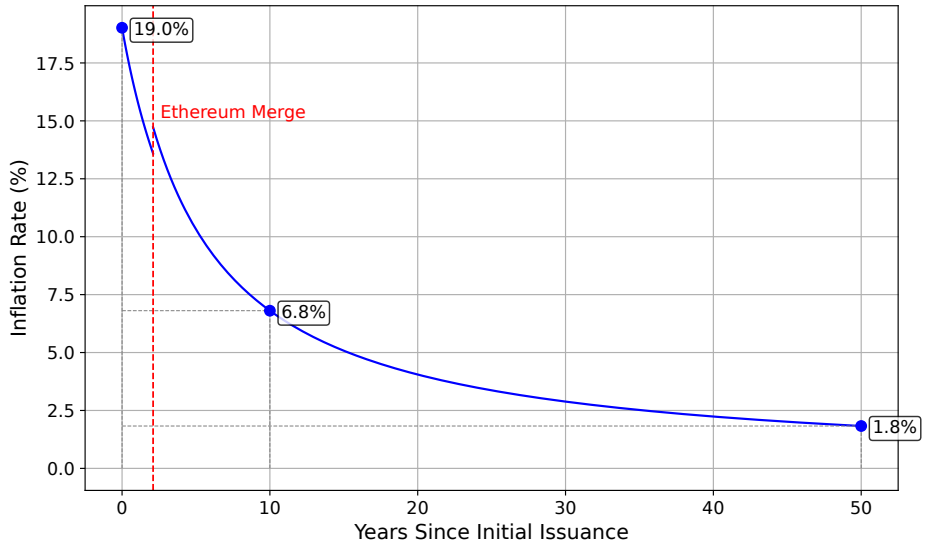

FIGURE 2. TON Inflation Rate Over Time

amount; rather, it functions as a minimum requirement to receive seigniorage. For details on TON Staking V1 and V2, please refer to the supplementary document provided in the references [4].

3.3.1. *TON staking V3.* TON Staking V3 is Tokamak Network's new token-economy model that distributes seigniorage based on the performance of L2 ecosystems. Figure 3 illustrates the overall structure of this model. While the previous V1/V2 models allocated rewards simply in proportion to the size of deposits, V3 defines Bridged TON as the primary performance metric of each L2 and uses it as the central criterion for distribution. This approach is intended to discourage artificial TVL inflation using external assets and provides a closer proxy for TON-native economic activity generated within the TON ecosystem.

As we can see in Figure 3, the model distributes staking rewards in proportion to each L2's measured performance, but applies diminishing marginal returns as performance increases. This encourages early ecosystem growth and prevents excessive seigniorage concentration by large participants. When aggregate L2 performance is low, effective seigniorage distribution decreases, which drives continuous growth and enables effective supply management based on performance. Validators also share in these performance-based rewards, and their incentives are aligned with overall ecosystem growth.

Core Tokenomics Rules. The core tokenomics of TON Staking V3 follows the rules below:

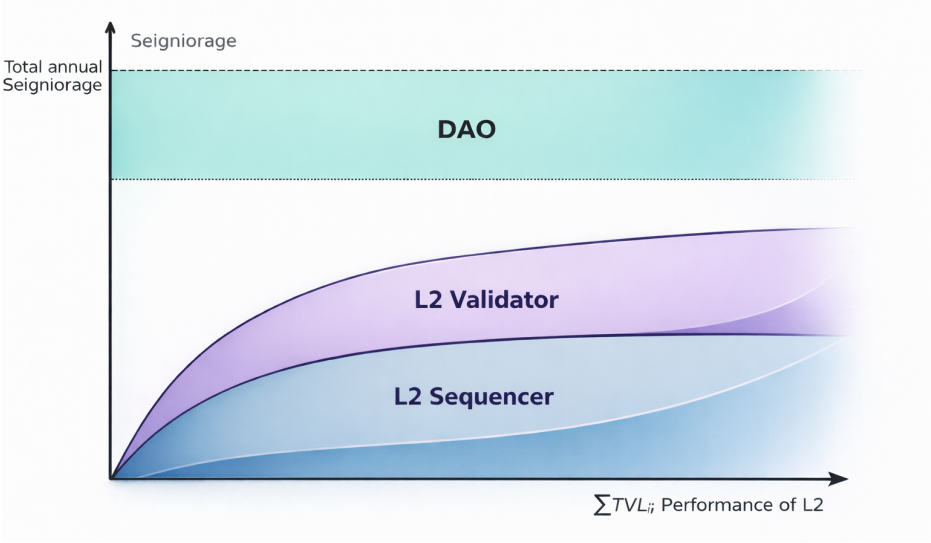

FIGURE 3. Seigniorage Allocation Structure in TON Staking V3

Rule 1 (Fixed Annual Seigniorage). The total annual seigniorage issuance A is fixed.

Rule 2 (DAO Fixed Allocation). A fixed portion of the annual seigniorage is allocated to the DAO:

$$S_{\text{DAO}} = d \cdot A \tag{7}$$

where $d \in (0, 1)$ is the DAO distribution parameter. Additionally, any undistributed seigniorage to L2s is also allocated to the DAO, which may use the funds for ecosystem reinvestment and public infrastructure development. Under Rule 1, this structure indirectly controls the effective supply actually released.

Rule 3 (Bridged TON as Performance Metric). L2 performance is measured by its Bridged TON amount. We define B_i as the amount of TON bridged to L2 i, and T_i as the amount of TON staked by the L2 sequencer on the L1 TON staking contract.

Rule 4 (Minimum Staking Requirement). Seigniorage allocation is not weighted by staking size; however, each L2 must satisfy the minimum staking requirement to be eligible for seigniorage in a given period:

$$T_i \geq \theta \cdot B_i \tag{8}$$

where $\theta \in (0, 1]$ is the minimum staking ratio parameter determined by the protocol. This requirement discourages disproportionate growth that increases TVL without adequate economic security and enforces a baseline level of security without using staking as a reward weight.

The seigniorage eligibility of each L2 i is expressed as an indicator function:

$$\mathbf{1}_i = \begin{cases} 1 & \text{if } T_i \geq \theta \cdot B_i \\ 0 & \text{otherwise} \end{cases} \tag{9}$$

The effective Bridged TON of an eligible L2 is defined as $\tilde{B}_i = \mathbf{1}_i \cdot B_i$. The total performance x is defined as the sum of effective Bridged TON across all L2s that meet the eligibility requirements during the given period:

$$x = \sum_i \tilde{B}_i = \sum_i \mathbf{1}_i \cdot B_i \tag{10}$$

Bridged TON and Staked TON are not sampled at strictly fixed intervals. Instead, the protocol uses the latest observed values captured through on-chain calls, and the evaluation mechanism is structured to closely track periodic measurements over time.

Seigniorage Allocation and Distribution. The total seigniorage allocated to the L2 ecosystem is determined using the hyperbolic saturation function [10]. This function imposes diminishing returns as performance increases, thereby preventing oversized L2s from capturing disproportionate rewards. The total L2 seigniorage $y(x)$ is defined as:

$$y(x) = L \cdot \frac{x}{k + x} = L \cdot \frac{\sum_i \tilde{B}_i}{k + \sum_i \tilde{B}_i} \tag{11}$$

where L is the upper bound of seigniorage allocated to L2s, defined as $L = (1 - d) \cdot A$, and k is the half-saturation point such that $y = L/2$ when $x = k$. The gap between $y(x)$ and the upper bound L in Figure 3 represents undistributed seigniorage, which flows to the DAO treasury. A smaller k results in faster initial growth and a more rapid decrease in marginal reward per unit of performance. This structure provides strong incentives during early growth while preventing excessive concentration of rewards among the largest L2s.

The seigniorage allocated to each L2 is determined by distributing the total reward $y(x)$ in proportion to performance. The seigniorage received by L2 i, denoted as S_i, is given by:

$$S_i = y(x) \cdot \frac{\tilde{B}_i}{x} \tag{12}$$

Rewards are divided between sequencers and validators according to a predefined ratio. Let α denote the validator distribution ratio. Let V_i denote the set of validators assigned to L2 i. The seigniorage received by validator j is:

$$v_j = \sum_{i:\, j \in V_i} \frac{\alpha \cdot S_i}{|V_i|} \tag{13}$$

where S_i is the seigniorage allocated to L2 i and $|V_i|$ is the number of validators in set V_i. The reward received by the sequencer of L2 i is:

$$o_i = (1 - \alpha) \cdot S_i \tag{14}$$

This structure distributes validator rewards in proportion to their assigned workload, as validators monitoring larger L2s bear greater verification responsibilities. If no validators are assigned to L2 i ($|V_i| = 0$), the validator portion $\alpha \cdot S_i$ is allocated to the DAO treasury. This design ensures that not only sequencers but also validators participating through the RAT (Randomized Attention Test) mechanism are included in the performance-driven reward model. This directly aligns the incentives of both sequencers and security contributors with the growth of the TON ecosystem.

In summary, TON Staking V3 provides a sustainable seigniorage distribution framework by measuring L2 performance through Bridged TON, mitigating scale bias via the saturation function, and enforcing a minimum staking requirement as a security mechanism. Considering the structural differences from V2, the transition should be implemented gradually to minimize disruption to existing stakers. This framework is an essential foundation for ensuring that a TON-centric multi-rollup environment grows in a self-sustaining and stable manner over the long term.

Acknowledgement

The authors would like to acknowledge Jason, Thomas, Dieu-Huyen Nguyen, HyukSang Jo for insightful discussions and review comments. We also acknowledge Monica for figure design and visual production.

References

[1] Eli Ben-Sasson, Iddo Bentov, Yinon Horesh, and Michael Riabzev, *Scalable, transparent, and post-quantum secure computational integrity*, CRYPTO, 2018.

[2] Vitalik Buterin, *An incomplete guide to rollups*, Vitalik Buterin's website, 2021, Accessed: 2025-12-04.

[3] Vitalik Buterin and Danny Ryan, *Ethereum merge: The transition to proof-of-stake*, Ethereum Foundation Blog (2022), Accessed: 2025-12-04.

[4] Kevin Jeong and Wyatt Park, *Tokamak layer 2 (l2) cryptoeconomics*, White paper, Tokamak Network Pte. Ltd., June 2023, First published June 2023, Accessed: 2025-12-04.

[5] Harry Kalodner, Steven Goldfeder, Xiaoqi Chen, Sharon Weinberg, and Edward W. Felten, *Arbitrum: Scalable, private smart contracts*, Proceedings of the 29th USENIX Security Symposium (Boston, MA, USA), USENIX Association, August 2020, pp. 1353–1370.

[6] Suhyeon Lee, Dieu-Huyen Nguyen, and Yeongju Bak, *Randomized attention test design for validator monitoring in optimistic rollups*, arXiv preprint arXiv:2505.24393 (2025), Version 3. Accessed: 2025-12-04.

[7] Suhyeon Lee, Dieu-Huyen Nguyen, and Donghwan Lee, *(im)possibility of incentive design for challenge-based blockchain protocols*, December 2025.

[8] Jiasun Li, *On the security of optimistic blockchain mechanisms*, Available at SSRN 4499357 (2023).

[9] Loi Luu, Jason Teutsch, Raghav Kulkarni, and Prateek Saxena, *Demystifying incentives in the consensus computer*, Proceedings of the 22nd acm sigsac conference on computer and communications security, 2015, pp. 706–719.

[10] Leonor Michaelis and Maud Menten, *Die kinetik der invertinwirkung*, Biochemische Zeitschrift (1913).

[11] Ertem Nusret Tas, John Adler, Mustafa Al-Bassam, Ismail Khoffi, David Tse, and Nima Vaziri, *Accountable safety for rollups*, arXiv preprint arXiv:2210.15017 (2022).

[12] Truebit Team, *Truebit unchained: Transparency powers the new era of verification*, Tech. report, Truebit, 2024.

[13] Jason Teutsch and Christian Reitwießner, *A scalable verification solution for blockchains*, 2019.