Tokamak layer 2(L2) Cryptoeconomics

Authors

- Kevin Jeong (kevin@tokamak.network)
- Wyatt Park (wyatt@tokamak.network)

Contents

Background summary

1. Tokamak Network Pte. Ltd. (the "Company") has developed a protocol utilizing the Layer 2 (L2) Optimistic Rollup scaling solution that will resolve the scalability problems of decentralized applications in Ethereum (L1) ("Tokamak Network"). The Tokamak Network will also provide an environment that will allow easy deployment of applications that was not possible to implement on the Ethereum blockchain due to its inherent performance and functional limitations.

2. The Tokamak Network has the following features/functions:

   Overview

   a. It is a L2 protocol designed to address the scalability problems of the Ethereum blockchain (due to a limited number of transactions per second and gas costs) by allowing users to first process transactions off the Ethereum chain, and subsequently have the transactions published on-chain in batches.

   Block verification

   b. Under the Optimistic Rollup approach, users submit transactions to "Sequencers" (as defined in Section 1 below), which are nodes responsible for processing transactions on the optimistic rollup. The Sequencer aggregates transactions, compresses the underlying data, and publishes the block on Ethereum.

   c. Sequencers are required to lock as "Sequencer collateral" (as defined in Section 1 below) a certain minimum number of Tokens (as further described below) as a form of a bond to dis- incentivize dishonesty as such bond can be slashed if the Sequencer posts an invalid block or builds on an old-but-invalid block (even if their block is valid). Sequencers are rewarded by the Tokamak Network with seigniorage (i.e. newly minted Tokens) for their services, the quantum of awards being in proportion to the growth of the corresponding L2 (growth being calculated on the basis of the growth of the total supply of Tokens on the Tokamak Network). However, in addition to seigniorage, different Sequencers may have different fee policies for how they are to be remunerated by users for their services (for example, in Tokens or in other cryptocurrencies).

   d. Under the Optimistic Rollup approach, after a rollup batch of

transactions are submitted by an Sequencer for publishing on the Ethereum blockchain, there is a time window/challenge period (called the "DTD", as defined in Section 1 below) of 7 to 14 days where users can "Challenge" (as defined in Section 1 below) the results of a transaction by computing fraud proofs (subject to them also providing Tokens in the form of "minimum challenge costs" (as described in Section 3.1.2 below). In the event where a particular Sequencer is Challenged, depending on whether the batch was validly submitted, the Sequencer or the challenger will lose their Sequencer collateral or minimum challenge costs respectively, and the winning party will obtain the losing party's slashed Tokens.

e. Users who are not Sequencers nor challengers (i.e. they themselves are not involved in either providing the service of processing transactions or computing fraud proofs), can also take part the block verification process by "supporting" the Sequencer or a challenger through similarly submitting Tokens to be locked up as minimum challenge costs, and in doing so can share in the rewards (i.e, seigniorage and/or slashed Tokens) and penalties (i.e the risk of slashing in the event of an invalid challenge/submission) which would have been obtained by the Sequencer or challenger respectively for their participation in block verification activities. For the avoidance of doubt, the act of "supporting" the Sequencer or the challenger is a proactive step a user has to take. A user can remain a passive Tokenholder on the Tokamak Network and not participate as a supporter in any of the challenges. The Tokens submitted to be locked up in this matter are intended to be for the purposes of encouraging active participation in the Tokamak Network and will not be used or monetized by the Company during such period that they are locked up.

f. Notwithstanding the above, to encourage active participation on the Tokamak Network's block verification activities, if a user on the Tokamak Network has staked Tokens but does not participate in such block verification process (i.e. not operating as a Sequencer, a challenger, or supporting either of them in a challenge), a portion of their staked Tokens will be slashed.

Fast withdrawals and liquidity providers

g. As part of the Optimistic Rollup protocol, in order to have transferred assets from L1 into L2, a user would have had to transfer its L1 assets to a token bridge, which is a smart contract that will lock the asset and communicate with a L2 – based Sequencer for such Sequencer to then relay the instructions to a token bridge on L2 to mint a corresponding amount of the same asset (in a wrapped form) on the L2 layer.

h. If a user initiates a transaction to withdraw assets locked on the

Ethereum layer (L1), the reverse process occurs. The user will deposit the corresponding L2 assets and submit a withdrawal request to the L2 token bridge, which will then have to be processed by the Sequencer (and would be subject to the abovementioned DTD period). If there is no successful Challenge during the DTD period, the withdrawal request will be relayed by the Sequencer to the L1 token bridge where the relevant assets will be released on the L1 layer and the corresponding assets on the L2 token bridge will be burnt.

i. Due to the above DTD period, the Tokamak Network permits users to act as fast withdrawal service providers who can who can take over as the recipient on the pending withdrawal request and pay the user on the L1 layer (in exchange for a fee), to enable a user to quickly exit the L2 without waiting through the challenge period. The Company itself does not carry out the role of a fast withdrawal service provider.

j. In support of the above, other than being able to act as fast withdrawal service providers themselves, users may also stake Tokens on the L1 layer to provide liquidity to the abovementioned fast withdrawal service providers, who may develop their own remuneration structures for rewarding stakers.

3. The Tokens is the native token of the Tokamak Network. It can be used for the following purposes:

   a. Potentially as fees payable to Sequencers on the Tokamak Network;
   b. To be provided as Sequencer collateral and/or minimum challenge costs, in relation to block verification processes (either as a Sequencer, a challenger, or a user supporting either of them in challenges)
   c. To be used by a user to provide fast withdrawal services, or staked on the L1 layer to other fast withdrawal service providers.

4. Tokens were previously available for purchase directly from the Company during a token generation event which is no longer running. However, they are currently obtainable by users of the Tokamak Network solely (i) through rewards by participating in the block verification processes (either as an Sequencer, a challenger, or a user supporting either of them); and (ii) by purchasing them from a third-party cryptocurrency exchange, to the extent that Tokens are made available on such third-party cryptocurrency exchanges.

5. Tokens cannot be redeemed or sold to the Company in exchange for fiat or other forms of cryptocurrencies.

6. A holder of a Token, by virtue of owning a Token, will not have any direct or indirect ownership of the assets of the Company.

7. While Tokens grant certain voting rights to holders, these rights will be limited to the elections and proposals conducted on-chain ("On-chain Voting Rights") and are not the same rights given to members/shareholders

of the Company, or voting rights concerning the management decisions of the Company (for example, decisions relating to changes in share capital, directors, the constitution, or dividends of the Company) nor any rights to the profit or revenue of the Tokamak Network or the Company. The On-chain Voting Rights shall be limited to voting on matters related to: (i) network upgrades and improvements; (ii) community proposals to allocate funds or resources to specific projects or initiatives of the Tokamak Network; (iii) changes to the Tokamak Network protocol; (iv) inclusion of support of other tokens on the Tokamak Network; and (v) changes to the governance structure of the Tokamak Network.

0. TL;DR

Layer 2 (L2) is a technology that emerged to complement the slower Layer 1 (L1) by processing transactions in L2 and relying on L1 for the validity of such transactions. Technologies such as Optimistic rollup, ZK (Zero-Knowledge) rollup, and Validium fall under this category. Currently, protocols that utilize Optimistic rollup like Arbitrum and Optimism hold about 80% of the L2 market. In Optimistic rollup, a bundle of L2 transactions is submitted to L1 and is considered valid unless users raise issues.

The Tokamak Network, based on Optimism, aims to foster a stable environment for the creation of on-demand L2 blockchains. We have been focusing on maximizing the utilities of TON to be competitive compared to other protocols using Optimistic rollup. For example, in a previous study, we explored how newly issued TON can help with L2 growth and establish native tokens as an L2 fee token.

In this paper, we will discuss further expanding the use of TON in the L2 environment by upgrading the existing staking service. As previously mentioned, TON seigniorage can facilitate L2 growth by rewarding sequencers' performances. It can alleviate the L2 fee token dilemma and thus lay the foundation for native tokens to be used as an L2 fee token. Consequently, L2 blockchains within the Tokamak Network can build independent economies and be on the path of sustainable growth. Additionally, TON, as a medium of rewards and punishment in challenges and fast withdrawals, can encourage TON stakers to take responsibility for L2 security. With appropriate rewards and penalties in a challenge, a more balanced staking incentive structure will motivate stakers to actively engage in verification tasks. Moreover, if we add the fast withdrawal service offered by stakers, a more robust L2 environment can be formed by mitigating the verifiers' dilemma.

1. Terminology

- **Staking**: Action of transferring tokens to the corresponding contract to ensure the network security in exchange for obtaining seigniorage. In the note, we discuss L1 staking only.
- **Unstaking**: Action of retrieving staked tokens
- **Seigniorage**: Difference between the nominal value and issuance costs of a currency; TON seigniorage is essentially the same as the amount of TON newly issued, given the zero issuance costs.
- **inflation**: Amount of currency newly issued / Total amount of currency issued
- **Deposit**: Action of transferring the balance of tokens in L1 into L2
- **Sequencer**: Entity who processes L2 transactions, creates L2 blocks, and submits relevant data to L1
- **Sequencer collateral**: Assets locked by sequencers as a collateral when opening L2
- **Challenge**: Action of verifying L2 transaction data submitted to L1 by any entity during DTD
- **DTD(Dispute Time Delay)**: Period during which any entity can verify L2 transaction data submitted to L1
- **Withdraw**: Action of transferring the balance of tokens in L2 into L1
- **Standard Withdrawal**: Withdrawal completed after DTD
- **Fast Withdrawal**: Withdrawal completed before DTD
- **Fraud proof**: Action of proving that the state transition by transactions is incorrect
- **Validity proof**: Action of proving that the state transition by transactions is correct

  In this note, unless defined differently, the terms 'token,' 'currency,' and 'asset' refer to TON. For example, 'staking' and 'deposits' refer to TON staking and TON deposits, respectively. It is to simplify the discussion as much as possible.

2. Seigniorage

TON seigniorage acts as a catalyst for the growth of L2 in the Tokamak Network. The continuous expansion of L2 provides a foundation for the native token to be used as a fee token.

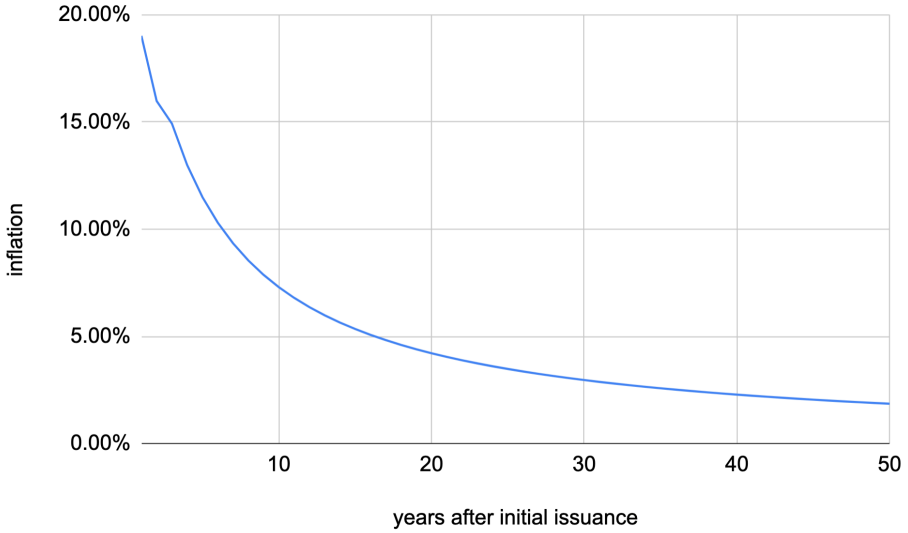
In a nutshell, TON promotes sustainable growth of L2 blockchains by enabling them to establish an economy less reliant on external factors.

2.1. Seigniorage generation

3.92 TON is issued for every block on Ethereum. Notably, as of the Merge (September 15th, 2022), the Ethereum block creation time changed, and the

annual amount of newly issued TON or annual seigniorage was affected accordingly. Before the Merge, given the average 13 seconds for Ethereum block creation time, seigniorage worth approximately 9,509,317 TON was generated. However, since the Merge reduced the block creation time to 12 seconds, the seigniorage increased to 10,301,760 TON after the Merge.

Given the initial issuance of 50,000,000 TON, the initial inflation is about 19.0% (9,509,317 / 50,000,000). The inflation drops to approximately 7.3% after 10 years and 1.9% after 50 years.



2.2. Seigniorage distribution

Distributing seigniorage refers to distributing newly issued TON to eligible entities, which helps balance the benefits and losses of an increased TON supply.

We assume the following properties to simplify the discussion:

1. Seigniorage is distributed periodically.
2. Only one L2 exists.

2.2.1. TON staking V1

The current staking service provided by Tokamak Network is called TON staking V1.

In this version, seigniorage is distributed in the following manner:

Stakers: $(\frac{S}{T} + W_S * \frac{T-S}{T}) * Seig$ **TON DAO:** $W_D * \frac{T-S}{T} * Seig$ **sTOS holders:** $W_P * \frac{T-S}{T} * Seig$

- T: Total TON supply

- S: Total amount of TON staked
- $Seig$: Seigniorage generated during a predetermined period
- W_S, W_D, W_P: Seigniorage weights for stakers / TON DAO / sTOS holders ($W_S + W_D + W_P \leq 1$)

If we assume $W_S = 1$, $W_D = W_P = 0$ to simplify the discussion, then all seigniorage will go to stakers.

Stakers: $(\frac{S}{T} + 1 * \frac{T-S}{T}) * Seig = Seig$ **TON DAO:** $0 * \frac{T-S}{T} * Seig = 0$ **sTOS holders:** $0 * \frac{T-S}{T} * Seig = 0$

2.2.2. TON staking V2

Once the L2 environment is established, TON Staking V1 will be upgraded to TON Staking V2. In this version, a sequencer will be able to receive seigniorage in proportion to L2 growth. For example, seigniorage can be distributed as follows:

Sequencer: $\frac{D+C}{T} * Seig = \frac{T_{L2}}{T} * Seig$ **Stakers:** $\frac{T-D-C}{T} * Seig = \frac{T-T_{L2}}{T} * Seig = \frac{T_{L1}}{T} * Seig$

- D: Total amount of TON deposited
- C: Sequencer collateral
- $T_{L2} \equiv D + C$: L2 TON supply
- $T_{L1} \equiv T - D - C = T - T_{L2}$: L1 TON supply

2.3. Sustainable growth of L2

TON seigniorage allows for the sustainable growth of L2 by facilitating its expansion and alleviating the L2 fee token dilemma.

2.3.1. Quantative/Qualitative growth of L2

2.3.1.1. Quantitative growth of L2 <=> increased seigniorage for sequencers Sequencers are motivated to increase seigniorage revenue by increasing deposits and collateral, which can result in significant growth of L2 as evidenced by the increase in Total Value Locked (TVL).

2.3.1.2. Qualitative growth of L2 <=> Qualitative improvement of seigniorage for sequencers The quality of seigniorage is also crucial. For example, if the seigniorage comes from only one depositor, it can be inherently unstable, as the revenue for the sequencer will drop significantly if the depositor withdraws.

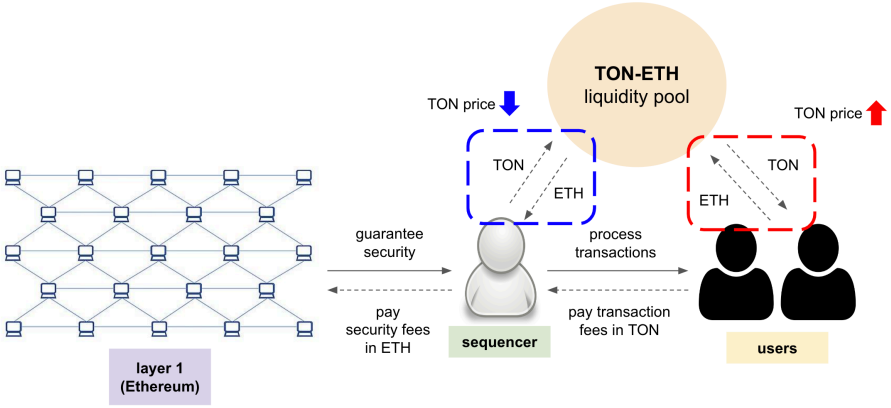
This is also related to the qualitative growth of L2. When liquidity is concentrated among a small number of depositors, it can discourage transactions, making L2 less attractive for users.

Therefore, sequencers will aim to bring more users to L2 to improve the quality of seigniorage revenue, which in turn leads to the qualitative growth of L2.

2.3.2. Alleviation of L2 fee token dilemma

The section refers to https://github.com/Onther-Tech/economics/blob/main/Tokamaklayer2.md.

We can address the long-term issue in L2, known as the "L2 fee token dilemma," by promoting both quantitative and qualitative growth of L2.



(*Source: How to unravel fee token dilemma in layer 2 by Wyatt Park*)

For example, the demand for TON can significantly increase when it is used as an L2 fee token, as users need TON for every transaction on L2. However, this is only one side of the coin. When L2 submits transaction data to L1 for security, a certain fee is incurred, and the fee can only be paid in ETH. This creates the L2 fee token dilemma as TON from L2 transaction fees may have to be sold to pay for L1 security fees.

Seigniorage distribution can alleviate this dilemma by encouraging sequencers to attract users to L2. Sequencers, driven by the potential seigniorage revenue, will bring users to L2, creating opportunities to diversify revenue streams such as through flexible fee policies or useful Dapps. As a result, sequencers will be able to cover L1 security fees without selling the native tokens (TON in this example) from L2 transaction fees.

3. Verification economics

In staking V2, TON contributes to not only the growth but also the security of L2. More specifically, it acts as a medium for rewards and penalties in challenges and helps to build a constant monitoring system by stakers. Furthermore, staking and staking-based fast withdrawals ameliorate the verifiers' dilemma and make L2 security even more robust.

3.1. Challenge

3.1.1. Overview

The security of the L2 layer heavily relies on a sequencer. In contrast to the L1, whose security is guaranteed by powerful economic incentives and multiple validators, the L2 is more vulnerable to attacks. Sequencers store L2 transaction data on the L1 to mitigate such instability. The challenge process ensures the validity of the data before it is committed to the L1. Anyone can challenge or raise issues against L2 transaction data during DTD.

However, relying solely on the generosity of random entities for security can be inherently unstable. Therefore, the upgraded staking service will include appropriate rewards and penalties to incentivize stakers to be deeply involved in challenges.

3.1.2. Procedure

In Tokamak Network, the challenge is expected to proceed as follows:

1. A sequencer submits the L2 block to L1.

2. After setting the 'minimum challenge costs' as collateral, a challenger engages in a Q&A process with the sequencer to verify the block. - The entity that gives the wrong answer or fails to respond within a predetermined period loses. - It takes 7 to 14 days(equal to or slightly shorter than DTD).

3. Non-challenger stakers can also participate in the challenge(Group Challenge). - It is possible to join the group challenge with the minimum challenge costs as collateral. - Stakers can support either the challenger or the sequencer.

4. Results

- If the challenger wins:
  - The challenger inherits the rights of the sequencer(including sequencer collateral).
  - There is no change in the assets of stakers supporting the challenger. However, depending on the situation, they may get a part of the sequencer collateral.
  - The sequencer gets disqualified.
  - Stakers supporting the sequencer lose the minimum collateral costs and have their stakes slashed.
  - The stakers not participating in the challenge get a portion of their stakes slashed.
- If the sequencer wins:
  - There is no change in the assets of the sequencer.
  - There is no change in the assets of the stakers supporting the sequencer.

  - The challenger and stakers supporting the challenger lose the minimum collateral costs, and their stakes get cut.
  - The stakers not participating in the challenge get a portion of their stakes slashed.

5. Others

- The sequencer will lose immediately if the following conditions hold:
  - No commits occur during DTD.

3.2. Fast Withdrawal

3.2.1. Overview

The fast withdrawal refers to the withdrawal completed before DTD.

As previously explained, anyone can initiate challenges and scrutinize the validity of L2 transactions during DTD. L2 transactions are not considered valid until the DTD ends. Therefore, users who request withdrawals cannot access their L1 assets corresponding to their L2 assets during the DTD. The fast withdrawal option can alleviate this inconvenience.

3.2.2. Source of liquidity

When users withdraw L2 assets, they are not allowed to access assets locked in L1. Therefore, obtaining liquidity for fast withdrawals, other than deposits, is necessary.

As the current staking service is updated, staked TON, in addition to external liquidity pools, can be used as the liquidity of fast withdrawals. Seigniorage or staking rewards and fast withdrawal fees will incentivize stakers to provide fast withdrawals. Additionally, staking rewards not affected by fast withdrawals during the DTD will reduce risks for stakers.

3.3. Verifiers' dilemma

> The section refers to Super-Simple Model in Optimistic Rollup in https://medium.com/onther-tech/optimistics-not-secure-enough-than-you-think-46bf93d80292.

3.3.1. Overview

Determining the appropriate levels of rewards and penalties in the challenge is crucial, as the "verifier's dilemma" arises in this situation. The verifier's dilemma occurs when no one will validate L2 transactions if the expected benefit of verification is not greater than that of non-verification.

In the Super-Simple Model of Optimistic Rollup, where a unique verifier who is also a stakeholder in the rollup can initiate a challenge, the expected payoffs of verification and non-verification are as follows:

Expected payoff of verification: $X * C + VR - VC$ **Expected payoff of non-verification:** $-X * L + (1 - X) * VR$

- C: Sequencer collateral; potential rewards for the verifier in the case of successful verification
- L: Assets deposited by the verifier in roll-up; potential rewards for sequencer in the case of failed verification.
- X: Probability of attack by the sequencer
- VC: Verification costs
- VR: Revenue from a unit of verification; benefits from safe L2 networks

The expected payoff of verification is greater than that of non-verification if $X > \frac{VC}{C+L+VR}$. Conversely, the verifiers' dilemma arises if $X \leq \frac{VC}{C+L+VR}$. Notably, It is difficult to completely eliminate the verifier's dilemma. For example, the dilemma will always occur if $VC \geq C + L + VR$ because $0 \leq X \leq 1 \leq \frac{VC}{C+L+VR}$. Conversly, a sequencer can find X_A that meets $0 < X_A \leq \frac{VC}{C+L+VR}$ if $VC < C + L + VR$, given that VC, C, L, VR are not negative.

Having multiple verifiers does not significantly change the discussion. Assuming multiple verifiers can initiate challenges, the expected payoffs of verification and non-verification for a specific verifier are as follows (Here C is evenly distributed among verifiers participating in the challenge):

Expected payoff of verification: $\frac{X*C}{N} + VR - VC$ **Expected payoff of non-verification:** $-X * Y * L + (1 - X * Y) * VR$

- N: Number of verifiers conducting verification including the verifier him/herself
- Y: Probability of no verifiers, except for the verifier him/herself, conducting verification

If no other verifiers perform verification ($N = 1, Y = 1$), the expected payoffs of verification and non-verification are as follows:

Expected payoff of verification: $X * C + VR - VC$ **Expected payoff of non-verification:** $-X * L + (1 - X) * VR$

The verifier is incentivized to validate L2 transactions if $X > \frac{VC}{C+L+VR}$, as we assumed with a unique verifier.

On the other hand, if all verifiers conduct verification ($N = NumberOfVerifiers = N_v, Y = 0$), the expected payoffs of verification and non-verification are as follows:

Expected payoff of verification: $\frac{X*C}{N_v} + VR$ - VC **Expected payoff of non-verification:** VR

The verifier is more likely to conduct verification if $X > \frac{N_v*VC}{C}$.

It can be inferred that the threshold value of X that would motivate some verifiers to conduct verification falls between $\frac{VC}{C+L+VR}$ and $\frac{N_v*VC}{C}$.

The conclusion can be summarized as follows:

1. $X > \frac{N_v * VC}{C}$: All the verifiers conduct verification
2. $\frac{VC}{C+L+VR} < X \leq \frac{N_v * VC}{C}$: Some verifiers may conduct verification
3. $X \leq \frac{VC}{C+L+VR}$: No verifiers conduct verification

The verifiers' dilemma arises regardless of X if $\frac{VC}{C+L+VR} \geq 1$, similar to the situation with a unique verifier. Moreover, even if $\frac{VC}{C+L+VR} < 1$, it is also not possible to completely eliminate the dilemma as a sequencer can adjust X to be less than or equal to $\frac{VC}{C+L+VR}$.

Therefore, the focus is on minimizing the maximum value of X that would discourage any verifiers from conducting verification, which is $\frac{VC}{C+L+VR}$ in the model above. The Tokamak Network aims to address this problem through staking and staking-based fast withdrawal mechanisms.

3.3.2. Mitigation of verifiers' dilemma

3.3.2.1. Basic verification model Assuming the unique verifier can initiate challenges, the expected payoffs of verification and non-verification in the Super-Simple Model of Optimistic Rollup are as follows:

Expected payoff of verification: $X * C + VR - VC$ **Expected payoff of non-verification:** $-X * L + (1 - X) * VR$

- C: Sequencer collateral; potential rewards for the verifier in the case of successful verification
- L: Assets deposited by the verifier in roll-up; potential rewards for sequencer in the case of failed verification.
- X: Probability of attack by the sequencer
- VC: Verification costs
- VR: Revenue from a unit of verification; benefits from safe L2 networks

It is economically rational for the verifier to validate L2 transactions if $X > \frac{VC}{C+L+VR}$. Conversely, the verifiers' dilemma arises if a sequencer reduces the X to be less than or equal to $\frac{VC}{C+L+VR}$. This remains the same in the case of multiple verifiers.

3.3.2.2. Staking verification model

- **Unique verifier**

With stakers now responsible for verification, meaning they become verifiers and can initiate challenges, the expected payoffs of verification and non-verification would change:

Expected payoff of verification: $X * C + VR - VC$ **Expected payoff of non-verification:** $-X * A * S + (1 - X) * VR$

- S: Staked TON

- A: Slashing rate of the staked TON

The only difference is that we put $A * S$, not L, in the expected payoff of non-verification. We do not consider staking rewards as they are irrelevant in analyzing payoffs related to verification.

The verifiers' dilemma occurs when $X \leq \frac{VC}{C+A*S+VR}$. Compared to the basic verification model, the staking verification model is more effective in mitigating the dilemma when $A * S > L$. It's worth noting that satisfying this inequality is realistic, as A is easier to control than L from the perspective of the protocol.

- **Multiple verfifiers**

With multiple stakers as verifiers, the expected payoffs of verification and non-verification for a specific verifier can be calculated as follows(Here C is evenly distributed among the challenger and the non-challenger stakers joining the group challenge):

Expected payoff of verification: $\frac{X*C}{N} + VR - VC$ **Expected payoff of non-verification:** $-X * A * S + (1 - X * Y) * VR$

- N: Number of verifiers conducting verification including the verifier him/herself
- Y: Probability of no verifiers, except for the verifier him/herself, conducting verification

It's worth noting that other verifiers cannot affect the outcome of a slashing event for a specific verifier. If the verifier fails to join a challenge, their staked TON will be slashed.

When no other verifiers conduct verification ($N = 1, Y = 1$), the expected payoffs of verification and non-verification can be calculated as follows:

Expected payoff of verification: $X * C + VR - VC$ **Expected payoff of non-verification:** $-X * A * S + (1 - X) * VR$

The verifier is incentivized to validate L2 transactions if $X > \frac{VC}{C+A*S+VR}$, similar to when there is only one verifier.

On the other hand, when all the verifiers conduct verification ($N = NumberOfVerifiers = N_v, Y = 0$), the expected payoffs of verification and non-verification can be calculated as follows:

Expected payoff of verification: $\frac{X*C}{N_v} + VR - VC$ **Expected payoff of non-verification:** $-X * A * S + VR$

The expected payoff of verification is greater than that of non-verification if $X > \frac{VC}{C/N_v+A*S}$.

It can be inferred that the threshold value of X that incentivizes some verifiers to conduct verification is between $\frac{VC}{C+A*S+VR}$ and $\frac{VC}{C/N_v+A*S}$.

The conclusion can be summarized as follows:

1. $X > \frac{VC}{C/N_v + A*S}$: All the verifiers conduct verification
2. $\frac{VC}{C+A*S+VR} < X \leq \frac{VC}{C/N_v+A*S}$: Some verifiers may conduct verification
3. $X \leq \frac{VC}{C+A*S+VR}$: No verifiers conducts verification

Higher A will force sequencers to lower X in order to make the L2 environment more favorable for attacks.

3.3.2.3. Staking & fast withdrawal verification model

- **Unique verifier**

The expected payoffs of verification and non-verification are updated when stakers not only perform verification tasks in a challenge but also offer fast withdrawals:

Expected payoff of verification: $X * C + VR - VC$ **Expected payoff of non-verification:** $-X * (A * S + FW) + (1 - X) * VR$

- FW: Staked TON used for fast withdrawals

Compared to the staking verification model, we add FW to the expected payoff of non-verification. We do not consider fast withdrawal fees because they are irrelevant in analyzing payoffs related to verification.

The verifiers' dilemma occurs if $X \leq \frac{VC}{C+A*S+VR+FW}$. In this scenario, the staker offering fast withdrawal is more likely to conduct verification, as FW lowers the expected payoff of non-verification. $(\frac{VC}{C+A*S+VR} > \frac{VC}{C+A*S+VR+FW})$

- **Multiple verifiers**

With multiple stakers acting as verifiers, the expected payoffs of verification and non-verification for a staker offering fast withdrawals can be calculated as follows(Here C is evenly distributed among the challenger and the non-challenger stakers joining the group challenge):

Expected payoff of verification: $\frac{X*C}{N} + VR - VC$ **Expected payoff of non-verification:** $-X * (A * S + FW) + (1 - X * Y) * VR$

- N: Number of verifiers conducting verification including the verifier him/herself
- Y: Probability of no verifiers, except for the verifier him/herself, conducting verification

Other verifiers have little impact on the expected payoff of non-verification for a staker offering fast withdrawals. The staked TON may be slashed regardless of verification by other verifiers. Additionally, fast withdrawal is typically completed before other verifiers begin their work, making it practically impossible to rely on them.

Using the same logic as previous models, the result can be summarized as follows:

1. $X > \frac{VC}{C/N_v+A*S+FW}$: All the verifiers conduct verification
2. $\frac{VC}{C+A*S+VR+FW} < X \leq \frac{VC}{C/N_v+A*S+FW}$: Some verifiers may conduct verification
3. $X \leq \frac{VC}{C+A*S+VR+FW}$: No verifiers conducts verification

Compared to the staking verification model, the maximum value of X, at which no verifiers conduct verification, is smaller. ($\frac{VC}{C+A*S+VR} > \frac{VC}{C+A*S+VR+FW}$)

3.3.2.4. Comparison among models

	Basic verification model	Staking verification model	Staking & fast withdrawal verification model
Maximum value of X causing verifiers' dilemma	$\frac{VC}{C+L+VR}$	$\frac{VC}{C+A*S+VR}$	$\frac{VC}{C+A*S+VR+FW}$

The staking verification model can more easily control verification incentives by adjusting A flexibly compared to the basic verification model. Additionally, the staking & fast withdrawal verification model can further mitigate the verifiers' dilemma by shrinking the expected payoff of non-verification with FW.

4. Utilities of TON

4.1. Sustainable growth of L2

TON incentivizes sequencers to contribute to the growth of L2 both quantitatively and qualitatively. Sequencers aim to attract capital from a large number of users in order to maximize stable seigniorage revenue, resulting in the expansion of L2. Once the user base is established, L2 can generate a revenue stream other than transaction fees through discretionary fee policies or useful Dapps. L2 can use a native token as a fee token without falling into the L2 fee token dilemma if such an additional cash flow covers L1 security fees.

As a result, L2 blockchains are able to build their economy with less influence from external factors.

4.2. Enhanced L2 security

First, as a medium for rewards and punishment in challenges, TON can implement a constant L2 monitoring system by stakers. Compared to traditional challenges, it is easier to design verification incentives because the protocol can flexibly adjust the expected payoffs for verification and non-verification for stakers.

Additionally, fast withdrawal by stakers can mitigate the verifiers' dilemma. This is because fast withdrawal transactions are unlikely to benefit from the verification by other verifiers. In other words, stakers who provide liquidity for fast withdrawals are motivated to carry out verification because of the harsher punishment for non-verification.

5. Validity Proof

We had assumed that there were no current technological means to prove the validity of L2 transactions. For example, using the fraud proof in Optimistic Rollup, the Tokamak Network will stimulate stakers to correct invalid transactions through challenges. However, as the validity proof (such as zero-knowledge proof) becomes more advanced, the verification process of L2 transactions will become simpler.

This will impact the utilities of TON. Firstly, it is notable that fast withdrawals may become less necessary, as verification will take less time. Therefore, there will be no need to provide incentives for fast withdrawals. On the other hand, regardless of the fraud proof or validity proof, challenges assisted by stakers can still be used. TON can keep contributing to L2 security as a medium for rewards and penalties in challenges. Furthermore, seigniorage distribution, which drives L2 expansion, is expected to maintain its role. TON seigniorage will be the foundation for sustainable growth of the L2 ecosystem by promoting both quantitative and qualitative growth of L2 and alleviating the L2 fee token dilemma.

6. Examples

6.1. Seigniorage distribution

We will use the following denotation in the example:

- T: Total TON supply
- S: Total amount of TON staked
- $Seig$: Seigniorage generated during a predetermined period
- D: Total amount of TON deposited
- C: Sequencer Collateral

Let's say a sequencer has just opened L2. For instance, if $Seig$ = 10 TON, T = 100 TON, D = 0 TON, and C = 20 TON, most of $Seig$ goes to stakers:

Sequencer: $\frac{D+C}{T} * Seig = \frac{0+20}{100} * 10 = 2$ TON **Stakers:** $\frac{T-D-C}{T} * Seig = \frac{100-0-20}{100} * 10 = 8$ TON

If the sequencer draws more depositors to L2, and as a result, D increases to 30 TON, $Seig$ is redistributed:

Sequencer: $\frac{D+C}{T} * Seig = \frac{30+20}{100} * 10 = 5$ TON **Stakers:** $\frac{T-D-C}{T} * Seig = \frac{100-30-20}{100} * 10 = 5$ TON

As the L2 TVL grows from 20 TON to 50 TON, the seigniorage for the sequencer increases from 2 TON to 5 TON.

The sequencer will try to raise D to 50 TON if the income generated from it (other than L2 transaction fees) is sufficient to cover L1 security fees.

Sequencer: $\frac{D+C}{T} * Seig = \frac{50+20}{100} * 10 = 7$ TON **Stakers:** $\frac{T-D-C}{T} * Seig = \frac{100-50-20}{100} * 10 = 3$ TON

An additional 2 TON is added to the seigniorage for the sequencer. Plus, the sequencer does not need to sell the native tokens from L2 transaction fees, thanks to the additional cash flow from increased deposits. This allows us to overcome the L2 fee token dilemma.

6.2. Verification economics

6.2.1. Challenge

We will use the folliwng denotation in the example: - C: Sequncer Collateral - S_A, S_B, S_C: TON staked by staker A, B, and C, respectively - $MinChal$: Mininum challege costs - A: Slashing rate

Let's think about a hypothetical L2 whose security relies on stakers A, B, and C. We assume $C = 1000$ TON, $S_A = 200$ TON, $S_B = 300$ TON, $S_C = 500$ TON, $MinChal = 100$ TON, and $A = 30\%$.

If the sequencer executes an attack using invalid transactions, stakers can either ignore it or initiate a challenge. The change in assets of each entity would be as follows if no challenge occurs:

Sequencer: 0 TON **Staker A:** $-S_A * A = -200 * 0.3 =$ -60 TON **Staker B:** $-S_B * A = -300 * 0.3 =$ -90 TON **Staker C:** $-S_C * A = -500 * 0.3 =$ -150 TON

If staker A runs a challenge and staker B supports it, while staker C does not participate in the challenge, the change in assets of each entity would be as follows:

Sequencer: $-C =$ -1000 TON **Staker A:** $+C = +1000$ TON **Staker B:** +0 TON **Staker C:** $-S_C * A = -500 * 0.3 =$ -150 TON

If staker C decides to join the challenge but chooses the wrong side, the bigger loss cannot be avoided:

Sequencer: $-C =$ -1000 TON **Staker A:** $+C = +1000$ TON **Staker B:** +0 TON **Staker C:** $-MinChal - S_C * A = -100 - (500 * 0.3) =$ -250 TON

As you can see from the results, appropriate rewards and punishments can encourage behaviors that benefit the protocol. Firstly, it is possible to receive

rewards if you can identify the malicious actions of a sequencer like staker A. Conversely, the stakes of all stakers can be slashed if no one initiates a challenge. Additionally, even if someone initiates a challenge, you can still lose a portion of your stake TON if you are absent from a challenge like staker C. Lastly, in the case of selecting the wrong side in a challenge, consequences can be even more serious.

6.2.2. Verifiers' dilemma

We assume a unique verifier in the examples below to simplify the discussion. As previously stated, the conclusion remains unchanged even when multiple verifiers exist.

6.2.2.1. Basic verification model The expected payoffs of verification and non-verification in Super-Simple Model in Optimistic Rollup are as follows:

Expected payoff of verification: $X * C + VR - VC$ **Expected payoff of non-verification:** $-X * L + (1 - X) * VR$

- C: Sequencer Collateral; potential rewards for the verifier in the case of successful verification
- L: Assets deposited by the verifier in roll-up; potential rewards for sequencer in the case of failed verification.
- X: Probability of attack by the sequencer
- VC: Verification costs
- VR: Revenue from a unit of verification; benefits from safe L2 networks

The value of X that makes the expected payoff of verification and non-verification equal is $\frac{2}{3}$ if $C = 10$, $L = 10$, $VC = 20$, and $VR = 10$:

Expected payoff of verification: $\frac{2}{3} * 10 + 10 - 20 = -\frac{10}{3}$ **Expected payoff of non-verification:** $-\frac{2}{3} * 10 + (1 - \frac{2}{3}) * 10 = -\frac{10}{3}$

We can shrink the maximum value of X that precipitates the verifiers' dilemma by increasing either C or L. For instance, the value of X that makes the expected payoff of verification and non-verification equal falls to $\frac{1}{2}$ if we double C:

Expected payoff of verification: $\frac{1}{2} * 20 + 10 - 20 = 0$ **Expected payoff of non-verification:** $-\frac{1}{2} * 10 + (1 - \frac{1}{2}) * 10 = 0$

Similarly, the value of X that makes the expected payoff of verification and non-verification equal falls to $\frac{1}{2}$ if we double L:

Expected payoff of verification: $\frac{1}{2} * 10 + 10 - 20 =$ -5 **Expected payoff of non-verification:** $-\frac{1}{2} * 20 + (1 - \frac{1}{2}) * 10 =$ -5

Consequently, as C or L increases, the maximum value of X that causes the verifiers' dilemma drops, making L2 safer. However, it can be difficult for the protocol to control C or L.

6.2.2.2. Staking verification model The expected payoffs of verification and non-verification get modified as follows:

Expected payoff of verification: $X * C + VR - VC$ **Expected payoff of non-verification:** $-X * A * S + (1 - X) * VR$

- S: Staked TON
- A: Slahsing rate of the staked TON

The value of X that makes the expected payoff of verification and non-verification equal is $\frac{2}{3}$ if we assume $C = 10$, $VC = 20$, $VR = 10$, $A = 0.1$, and $S = 100$ ($L = 10 = 0.1 * 100 = A * S$):

Expected payoff of verification: $\frac{2}{3} * 10 + 10 - 20 = -\frac{10}{3}$ **Expected payoff of non-verification:** $-\frac{2}{3} * 0.1 * 100 + (1 - \frac{2}{3}) * 10 = -\frac{10}{3}$

The value of X that makes the expected payoff of verification and non-verification equal is $\frac{1}{2}$ if we double A.

Expected payoff of verification: $\frac{1}{2} * 10 + 10 - 20$ = -5 **Expected payoff of non-verification:** $-\frac{1}{2} * 0.2 * 100 + (1 - \frac{1}{2}) * 10$ = -5

We have the same result as the basic verification model with $L = 10$ and $L = 20$. However, because A is more easily controllable, it is much simpler to achieve an identical outcome.

6.2.2.3. Staking & fast withdrawal verification model With stakers offering fast withdrawals, the expected payoffs of verification and non-verification are updated as follows:

Expected payoff of verification: $X * C + VR - VC$ **Expected payoff of non-verification:** $-X * (A * S + FW) + (1 - X) * VR$

- FW: Staked TON used for fast withdrawals

The value of X that makes the expected payoff of verification and non-verification equal is $\frac{2}{13}$ if we assume $C = 10$, $VC = 20$, $VR = 10$, $A = 0.1$, $S = 100$, and $FW = 100$:

Expected payoff of verification: $\frac{2}{13} * 10 + 10 - 20 = -\frac{110}{13}$ **Expected payoff of non-verification:** $-\frac{2}{13} * (0.1 * 100 + 100) + (1 - \frac{2}{13}) * 10 = -\frac{110}{13}$

It is safer than the staking verification model. ($\frac{2}{3} > \frac{2}{13}$)

The value of X that makes the expected payoff of verification and non-verification equal drops to $\frac{2}{14} = \frac{1}{7}$ if we double A:

Expected payoff of verification: $\frac{1}{7} * 10 + 10 - 20 = -\frac{60}{7}$ **Expected payoff of non-verification:** $-\frac{1}{7} * (0.2 * 100 + 100) + (1 - \frac{1}{7}) * 10 = -\frac{60}{7}$

Again, it is safer than the staking verification model. ($\frac{1}{2} > \frac{1}{7}$)

6.2.2.4. Comparison among models Assuming $C = 10$, $L = 10$, $VC = 20$, $VR = 10$, $A = 0.1$, $S = 100$, and $FW = 100$, the maximum value of X triggering the verifiers' dilemma in each model is as follows:

	Basic verification model	Staking verification model	Staking & fast withdrawal verification model
Maximum value of X causing verifiers' dilemma	$\frac{1}{2}$	$\frac{1}{2}$	$\frac{1}{7}$
		more controllable parameters	more controllable parameters

7. References

https://github.com/Onther-Tech/economics/blob/main/Tokamaklayer2.md

https://medium.com/onther-tech/optimistics-not-secure-enough-than-you-think-46bf93d80292

8. Appendix

8.1. Disclaimer

This Economic paper and other documents distributed in relation hereto are used for the development and application of the Tokamak Network, and the material contained herein is for informational purposes only and may change in the future. Accordingly, please read this entire section carefully. If you are in any doubt as to the action you should take, please consult your legal, financial, tax or other professional advisor(s).

8.1.1. Legal Statement

(a) This Economic paper ("Economic paper"), in its current form, is circulated for general information purposes only in relation to the protocol and applications described in the Economic paper ("Protocol") as presently conceived and is subject to review and revision. Please note that this Economic paper is a work in progress and the information in this Economic paper is current only as of the date on the cover hereof. Thereafter, the information, including information concerning Tokamak Network Pte Ltd's (the "Company") intentions, business operations and financial condition (if applicable) may have changed. We reserve the right to change, modify, add or delete parts of this Economic paper or website without notice for any reason or at any time.

(b) No person is bound to enter into any contract or binding legal commitment in relation to the sale and purchase of the tokens native to the Protocol ("TON Token" or "Token") (as defined below) and no payment is to be accepted on the basis of this Economic paper. Any sale and purchase of the Token will be governed by a legally binding agreement, the details of which will be made available separately from this Economic paper. In the event of any inconsistencies between the abovementioned agreement and this Economic paper, the former shall prevail.

(c) This Economic paper does not constitute or form part of any opinion on any advice to sell, or any solicitation of any offer by the issuer/distributor/vendor of the Token to purchase any Token nor shall it or any part of it nor the fact of its presentation form the basis of, or be relied upon in connection with, any contract or investment decision.

(d) The Tokens are not intended to constitute securities, units in a business trust, or units in a collective investment scheme, each as defined under the Securities and Futures Act (Cap. 289) of Singapore, or its equivalent in any other jurisdiction. Accordingly, this Economic paper therefore, does not, and is not intended to, constitute a prospectus, profile statement, or offer document of any sort, and should not be construed as an offer of securities of any form, units in a business trust, units in a collective investment scheme or any other form of investment, or a solicitation for any form of investment in any jurisdiction.

(e) No Token should be construed, interpreted, classified or treated as enabling, or according any opportunity to, purchasers to participate in or receive profits, income, or other payments or returns arising from or in connection with the Protocol or the Token, or to receive sums paid out of such profits, income, or other payments or returns.

(f) This Economic paper or any part hereof may not be reproduced, distributed or otherwise disseminated in any jurisdiction where the offer/distribution of digital tokens in the manner set out this Economic paper is regulated or prohibited. Receipt of the Economic paper does not guarantee or indicate any eligibility or guarantee of participation in the project described in the Economic paper.

(g) No regulatory authority has reviewed, examined or approved of any of the information set out in this Economic paper. No such action has been or will be taken in any jurisdiction.

(h) This Economic paper contains the perspective and view of the Company which does not reflect the policies or positions of public authorities such as governments, quasi-governments, authorities or regulators in any jurisdiction. The information contained in the Economic paper is based on information obtained from reliable sources, and the Company does not guarantee its accuracy or completeness.

(i) References to specific companies and platforms in the Economic paper are for general reference and/or comparison purposes only. The use of the name of the enterprise or platforms and registered trademarks does not signify affiliation or endorsement of the party concerned.

(j) Where you wish to or have purchased any Token, the Tokens are not to be construed, interpreted, classified or treated as: (a) any kind of currency other than cryptocurrency; (b) debentures, stocks or shares issued by any entity; (c) rights, options or derivatives in respect of such debentures, stocks or shares; (d) rights under a contract for differences or under any other contract with the purpose or pretended purpose to secure a profit or avoid a loss; or (e) units or derivatives in a collective investment scheme or business trust, or any other type of securities.

(k) If the materials on Tokamak Network other than the Economic paper conflict with it, the Economic paper should take priority.

8.1.2. Restrictions on Distribution and Dissemination

(a) The distribution or dissemination of this Economic paper or any part thereof may be prohibited or restricted by the laws or regulatory requirements of any jurisdiction. In the case where any restriction applies, you are to inform yourself about, to obtain legal and other relevant advice on, and to observe, any restrictions which are applicable to your possession of this Economic paper or such part thereof (as the case may be) at your own expense and without liability to the Company or its representatives, agents, and related companies ("Affiliates").

(b) Persons to whom a copy of this Economic paper has been distributed or disseminated, provided access to or who otherwise have the Economic paper in their possession shall not circulate it to any other persons, reproduce or otherwise distribute this Economic paper or any information contained herein for any purpose whatsoever nor permit or cause the same to occur.

8.1.3. Disclaimer of Liability

(a) The Token, the Protocol and related services provided by the Company and its affiliates are provided on an "as is" and "as available" basis. The Company and its Affiliates do not grant any warranties or make any representation, express or implied or otherwise, as to the accessibility, quality, suitability, accuracy, adequacy, or completeness of the Token, the Protocol or any related services provided by the Company and its Affiliates, and expressly disclaim any liability for errors, delays, or omissions in, or for any action taken in reliance on, the Token, the Protocol and related services provided by the Company and its Affiliates.

(b) The Company, its Affiliates and its directors, officials and employees do not make or purport to make, and hereby disclaim, any representation,

warranty or undertaking in any form whatsoever to any entity or person, including any representation, warranty or undertaking in relation to the truth, accuracy and completeness of any of the information set out in this Economic paper.

(c) To the maximum extent permitted by the applicable laws and regulations, the Company and its Affiliates shall not be liable for any indirect, special, incidental, consequential or other losses of any kind, in tort, contract or otherwise (including but not limited to loss of revenue, income or profits, and loss of use or data), arising out of or in connection with any acceptance of or reliance on this Economic paper or any part thereof by you.

8.1.4. Cautionary Note on Forward-Looking Statements

(a) Certain information set forth in this Economic paper includes forward-looking information regarding the future of the project, future events and projections. These statements are not statements of historical fact and may be identified by but not limited to words and phrases such as "will", "estimate", "believe", "expect", project", "anticipate", or words of similar meaning. Such forward-looking statements are also included in other publicly available materials such as presentations, interviews, videos etc., information contained in this Economic paper constitutes forward-looking statements including but not limited to future results, performance, or achievements of the Company or its Affiliates.

(b) The forward-looking statements involve a variety of risks and uncertainties. These statements are not guarantees of future performance and no undue reliance should be placed on them. Should any of these risks or uncertainties materialize, the actual performance and progress of the Company or its Affiliates might differ from expectations set by the forward-looking statements. The Company or its Affiliates undertake no obligation to update forward-looking statements should there be any change in circumstances. By acting upon forward-looking information received from this Economic paper, the Company or its Affiliates' website and other materials produced by the Company or its Affiliates, you personally bear full responsibility in the event where the forward-looking statements do not materialize.

(c) As of the date of this Economic paper, the Protocol has not been completed and is not fully operational. Any description pertaining to and regarding the Protocol is made on the basis that the Protocol will be completed and be fully operational. However, this paragraph shall in no way be construed as providing any form of guarantee or assurance that the Protocol will eventually be completed or be fully operational.

8.1.5. Potential Risks

By purchasing, holding and using the Tokens, you expressly acknowledge and assume the risks set out in this section if any of these risks and uncertainties develops into actual events, the business, financial condition, results of operations and prospects of the Company or its Affiliates may be materially and adversely affected. In such cases, you may lose all or part of the value of the Token.

Risks Relating to the Tokens (a) There may not be a public or secondary market available for the Tokens

I. The Tokens are intended to be native tokens to be used on the Protocol, and the Company and its Affiliates have not and may not actively facilitate any secondary trading or external trading of Tokens. In addition, there is and has been no public market for the Tokens and the Tokens are not traded, whether on any cryptocurrency exchange or otherwise. In the event that the Tokens are traded on a cryptocurrency exchange, there is no assurance that an active or liquid trading market for the Tokens will develop or if developed, be sustained. There is also no assurance that the market price of the Tokens will not decline below the purchase amount paid for the Tokens, which is not indicative of such market price.

II. A TON Token is not a currency issued by any central bank or national, supra-national or quasi-national organization, nor is it backed by any hard assets or other credit. The Company and its Affiliates are not responsible for nor do they pursue the circulation and trading of the Tokens on the market. Trading of the Tokens merely depends on the consensus on its value between the relevant market participants, and no one is obliged to acquire any Token from any holder of the Token, including the purchasers of the Tokens, nor does anyone guarantee the liquidity or market price of the Tokens to any extent at any time. Accordingly, the Company and its Affiliates cannot ensure that there will be any demand or market for the Tokens, or that the price upon which the Tokens were purchased is indicative of the market price of the Tokens if they are made available for trading on a cryptocurrency exchange.

Risks Relating to the Company, its Affiliates and the Protocol (a) Limited availability of sufficient information

The Protocol is still at an early development phase as of the date of this Economic paper. Its governance structure, purpose, consensus mechanism, algorithm, code, infrastructure design and other technical specifications and parameters may be updated and changed frequently without notice. While this Economic paper contains the key information currently available in relation to the Protocol, it is subject to adjustments and updates from time to time, as announced on the Company's website at Tokamak Network Official Twitter. Users of the Protocol will not have full access to all the information relevant to

the Tokens and/or the Protocol. Nevertheless, it is anticipated that significant milestones and progress reports will be announced on the Company's website at Tokamak Network Official Twitter.

(b) The digital assets raised in the sale of the Tokens are exposed to the risks of theft

Whilst the Company and its Affiliates will make every effort to ensure that any cryptocurrencies received from the sale of Tokens are securely held through the implementation of security measures, there is no assurance that there will be no theft of the cryptocurrencies as a result of hacks, mining attacks, sophisticated cyber-attacks, distributed denials of service or errors, vulnerabilities or defects on such blockchain addresses, or any other blockchain, or otherwise. Such events may include, for example, flaws in programming or source code leading to exploitation or abuse thereof. In such event, even if the sale of Tokens is completed, the Company and its Affiliates may not be able to receive the cryptocurrencies raised and the Company and its Affiliates may not be able to utilize such funds for the development of the Protocol, and the launch of the Protocol might be temporarily or permanently curtailed. As such, the issued Tokens may hold little worth or value. The Tokens are uninsured, unless you specifically obtain private insurance to insure them. In the event of any loss or loss of value of the Tokens, you may have no recourse.

(c) The blockchain address(es) may be compromised and the digital assets may not be able to be retrieved

Blockchain address(es) are designed to be secured. However, in the event that the blockchain address(es) for the receipt of purchase amounts or otherwise are, for any reason, compromised (including but not limited to scenarios of the loss of keys to such blockchain address(es), the funds held at such blockchain address(es) may not be able to be retrieved and disbursed, and may be permanently unrecoverable. In such event, even if the sale of the Tokens is successful, the Company and its Affiliates will not be able to receive the funds raised and the Company and its Affiliates will not be able to utilize such funds for the development of the Protocol, and the implementation of the Protocol might be temporarily or permanently curtailed. As such, distributed Tokens may hold little worth or value.

(d) There is no assurance of any success of the Protocol and the Company and its Affiliates may cease the development, launch and operation of the Protocol.

I. The value of, and demand for, the Tokens hinges heavily on the performance of the Protocol. There is no assurance that the Protocol will gain traction after its launch and achieve any commercial success. The Protocol has not been fully developed, finalized and integrated and is subject to further changes, updates and adjustments prior to its launch. Such changes may result in unexpected and unforeseen effects on its projected appeal to users, and hence impact its

success. There are no guarantees that the process for creating the Tokens will be uninterrupted or error-free.

II. While the Company has made every effort to provide a realistic estimate, there is also no assurance that the any cryptocurrencies raised in the sale of Tokens will be sufficient for the development and integration of the Protocol. For the foregoing or any other reason, the development and integration of the Protocol may not be completed and there is no assurance that its systems, protocols or products will be launched at all. As such, distributed Tokens may hold little or no worth or value.

III. Additional reasons which may result in the termination of the development, launch or operation of the Protocol includes, but is not limited to, (aa) an unfavorable fluctuation in the value of cryptographic and fiat currencies, (bb) the inability of the Company and its Affiliates to establish the Protocol or the Tokens' utility or to resolve technical problems and issues faced in relation to the development or operation of the Protocol or the Token, the failure of commercial relationships, (cc) intellectual property disputes during development or operation, and (dd) changes in the future capital needs of the Company or its Affiliates and the availability of financing and capital to fund such needs. For the aforesaid and other reasons, the Protocol may no longer be a viable project and may be dissolved or not launched, negatively impacting the Protocol and the potential utility and value of issued TON Tokens.

(e) There may be lack of demand for the Protocol and the services provided, which would impact the value of the Tokens

I. There is a risk that upon launching of the Protocol, there is a lack of interest from consumers, merchants, advertisers, and other key participants for the Protocol and the services, and that there may be limited interest and therefore use of the Protocol and the Tokens. Such a lack of interest could impact the operation of the Protocol and the uses or potential value of the Tokens.

II. There is a risk of competition from alternative platforms/protocols that may have been established, or even from existing businesses which would target any segment of the potential users of the Protocol fulfilling similar demands, e.g. corporations targeting advertisers seeking purchase consumer data and market analysis. Therefore, in the event that the competition results in a lack of interest and demand for the Protocol, the services and the Tokens, the operation of the Protocol and Token value may be negatively impacted. r specialist as necessary before deciding whether to purchase TON tokens or participate in the Tokamak Network project.

(f) The Company and its Affiliates may experience system failures, unplanned interruptions in its network or services, hardware or software defects, security breaches or other causes that could adversely affect the Company or its Affiliates' infrastructure network, or the Protocol

I. The Company and its Affiliates are unable to anticipate or detect when there would be occurrences of hacks, cyber-attacks, mining attacks (including but not limited to double-spend attacks, majority mining power attacks and "selfish-mining" attacks), distributed denials of service or errors, vulnerabilities or defects in the Protocol, the Tokens, or any technology (including but not limited to smart contract technology) on which the Company, its Affiliates, the Protocol, the Tokens, rely on or the Ethereum Blockchain or any other blockchain. Such events may include, for example, flaws in programming or source code leading to exploitation or abuse thereof. The Company and its Affiliates may not be able to detect such issues in a timely manner, and may not have sufficient resources to efficiently cope with multiple service incidents happening simultaneously or in rapid succession.

II. Although the Company and its Affiliates will be taking steps against malicious attacks on its appliances or its infrastructure, which are critical for the maintenance of the Protocol and its other services, there can be no assurance that cyber-attacks, such as distributed denials of service, will not be attempted in the future, and that any of such security measures will be effective. Any significant breach of security measures or other disruptions resulting in a compromise of the usability, stability and security of the Company and its Affiliates' network or services, including the Protocol.

Risks Relating to the Participation in the Sale of Tokens (a) You may not be able to recover the purchase amount paid for the Tokens

Except as provided under any applicable terms of sale or prescribed by applicable laws and regulations, the Company is not obliged to provide you with a refund of any purchase amount. No promises of future performance or price are or will be made in respect to the Tokens, including promises of inherent value or continuing payments, and there is no guarantee that the Tokens will hold any particular value. Therefore, the recovery of the purchase amount may be impossible or may be subject to applicable laws and regulations.

(b) You may be subject to adverse legal and/or tax implications as a result of the purchase, distribution and use of the Tokens.

I. The legal character of cryptocurrency and cryptographic assets remain uncertain. There is a risk that the Tokens may be considered securities in certain jurisdictions, or may be considered to be securities in certain jurisdictions in the future. The Company and its Affiliates does not provide any warranty or guarantee as to how the Tokens will be classified, and each purchaser will bear all consequences of the Tokens being considered securities in their respective jurisdictions, and bear the responsibility of the legality, use and transfer of the Tokens in the relevant jurisdictions. II. Further, the tax treatment of the acquisition or disposal of such cryptocurrency or cryptographic assets might depend on whether they are classified as securities, assets, currency or otherwise. As the tax characterization of the Tokens remains indeterminate, you must seek

your own tax advice in connection with the purchase, acquisition or disposal of the Tokens, which may result in adverse tax consequences or tax reporting requirements for you.

(c) The loss or compromise of information relating to the purchaser wallet and your method of accessing the Protocol may affect your access to and possession of the Tokens

There is a risk that you may lose access to and possession of the Tokens permanently due to loss of unique personal ID used to access the Protocol, and other identification information, loss of requisite private key(s) associated with the purchaser wallet or vault storing the Tokens or any other kind of custodial or purchaser errors.

(d) Blockchains may face congestion and transactions may be delayed or lost. Most blockchains used for cryptocurrency transactions (e.g. Ethereum) are prone to periodic congestion during which transactions can be delayed or lost. Individuals may also intentionally spam the network in an attempt to gain an advantage in purchasing cryptographic tokens.

This may result in a situation where block producers may not include your purchase of the Tokens when you intend to transact, or your transaction may not be included at all.

Privacy and data retention issues. As part of any Token sales, the verification processes and the subsequent operation of the Protocol, the Company may collect personal information from you. The collection of such information is subject to applicable laws and regulations. All information collected will be used for purposes of the Token sales and operations of the Protocol, thus it may be transferred to contractors, service providers and consultants worldwide as appointed by the Company. Apart from external compromises, the Company and its appointed entities may also suffer from internal security breaches whereby their employees may misappropriate, misplace or lose personal information of purchasers. The Company may be required to expend significant financial resources to alleviate problems caused by any breaches or losses, settle fines and resolve inquiries from regulatory or government authorities. Any information breaches or losses will also damage the Company's reputations, thereby harming its long-term prospects.

Macro Risks (a) General global market and economic conditions may have an adverse impact on the Company and its Affiliates' operations and the use of the Protocol.

I. The Company and its Affiliates could be affected by general global economic and market conditions. Challenging economic conditions worldwide have from time to time, contributed, and may continue to contribute, to slowdowns in the information technology industry at large. Weakness in the economy may have

a negative effect on the Company and its Affiliates' business strategies, results of operations and prospects.

II. Suppliers on which the Protocol relies for servers, bandwidth, location and other services could also be negatively impacted by economic conditions that, in turn, could have a negative impact on the Company and its Affiliates' operations or expenses.

III. There can be no assurance, therefore, that current economic conditions or worsening economic conditions or a prolonged or recurring recession will not have a significant adverse impact on the Company and its Affiliates' business strategies, results of operations and prospects and hence the Protocol, which may in turn impact the value of the Tokens.

(b) The regulatory regime governing blockchain technologies, cryptocurrencies, Tokens, offering of Tokens, and the Protocol remain uncertain, and any changes, regulations or policies may materially adversely affect the development of the Protocol and the utility of the Tokens

I. Regulation of the Tokens, the offer and sale of Tokens, cryptocurrencies, blockchain technologies, and cryptocurrency exchanges is currently undeveloped or underdeveloped and likely to rapidly evolve. Such regulation also varies significantly among different jurisdictions, and is hence subject to significant uncertainty. The various legislative and executive bodies in different jurisdictions may in the future adopt laws, regulations, guidance, or other actions, which may severely impact the development and growth of the Protocol, the adoption and utility of the Tokens or the issue, offer, and sale of the Tokens by the Company. Failure by the Company and its Affiliates or users of the Protocol to comply with any laws, rules and regulations, some of which may not exist yet or are subject to interpretation and may be subject to change, could result in a variety of adverse consequences against the Company and its Affiliates, including civil penalties and fines.

II. Blockchain networks also face an uncertain regulatory landscape in many foreign jurisdictions. Various jurisdictions may, in the near future, adopt laws, regulations or directives that affect the Protocol, and therefore, the value of the Tokens. Such laws, regulations or directives may directly and negatively impact the operations of the Company and its Affiliates. The effect of any future regulatory change is impossible to predict, but such change could be substantial and could materially adverse to the development and growth of the Protocol and the adoption and utility of the Tokens.

III. To the extent that the Company and its Affiliates may be required to obtain licenses, permits and/or approvals (collectively, the "Regulatory Approvals") to carry out its business, including that of the creation of the Tokens and the development and operation of the Protocol, but are unable to obtain such Regulatory Approvals or if such Regulatory Approvals are

not renewed or revoked for whatever reason by the relevant authorities, the business of the Company and its Affiliates may be adversely affected.

IV. There is no assurance that more stringent requirements will not be imposed upon the Company and its Affiliates by the relevant authorities in the future, or that the Company and its Affiliates will be able to adapt in a timely manner to changing regulatory requirements. These additional or more stringent regulations may restrict the Company and its Affiliates' ability to operate its business and the Company and its Affiliates may face actions for non-compliance if it fails to comply with any of such requirements.

V. Further, should the costs (financial or otherwise) of complying with such newly implemented regulations exceed a certain threshold, maintaining the Protocol may no longer be commercially viable and the Company and its Affiliates may opt to discontinue the Protocol and/or the Tokens. Further, it is difficult to predict how or whether governments or regulatory authorities may implement any changes to laws and regulations affecting distributed ledger technology and its applications, including the Protocol and the Tokens. The Company and its Affiliates may also have to cease operations in a jurisdiction that makes it illegal to operate in such jurisdiction, or make it commercially unviable or undesirable to obtain the necessary regulatory approval(s) to operate in such jurisdiction. In scenarios such as the foregoing, the distributed Tokens may hold little or no worth or value.

(c) There may be risks relating to acts of God, natural disasters, epidemics, pandemics, wars, terrorist attacks, riots, civil commotions widespread communicable diseases and other events beyond the control of the Company and its Affiliates

Any sale of the Tokens and the performance of the Company, its Affiliates and/or the Protocol's activities may be interrupted, suspended or delayed due to acts of God, natural disasters, wars, terrorist attacks, riots, civil commotions, widespread communicable diseases, epidemics, pandemics and other events beyond the control of the Company and its Affiliates. Such events could also lead to uncertainty in the economic outlook of global markets and there is no assurance that such markets will not be affected, or that recovery from the global financial crisis would continue. In such events, the Company and its Affiliates' business strategies, results of operations and outlook may be materially and adversely affected, and the demand for and use of the Tokens and the Protocol may be materially affected. Further, if an outbreak of such infectious or communicable diseases occurs in any of the countries in which the Company, its Affiliates, and the participants of the Protocol have operations in the future, market sentiment could be adversely affected and this may have a negative impact on the Protocol and its community.

(d) Blockchain and cryptocurrencies, including the Tokens are a relatively new and dynamic technology. In addition to the risks high-

lighted herein, there are other risks associated with the purchase of, holding and use of the Tokens, including those that we cannot anticipate. Such risks may further materialize as unanticipated variations or combinations of the risks discussed herein.

8.1.6. No Further Information or Update

No person has been or is authorized to give any information or representation not contained in this Economic paper in connection with the Tokens, the Protocol, the Company or its Affiliates and their respective businesses and operations, and, if given, such information or representation must not be relied upon as having been authorized by or on behalf of the Company or its Affiliates.

8.1.7. Language

This Economic paper may be translated into other languages. If any disagreement should arise due to different language translations, the version in English will prevail.

8.1.8. Advice

No information in this Economic paper should be considered to be business, legal, financial or tax advice regarding the Token, the Protocol, the Company or its Affiliates. You should consult your own legal, financial, tax or other professional advisor(s) regarding the Token, the Company or its Affiliates and their respective businesses and operations. You should be aware that you may be required to bear the financial risk of any purchase of the Tokens for an indefinite period of time.