Validator Penalties, Slashing, and their Impact on Tokemak v2

Tokemak

Follow

Tokemak

--

Listen

Share

Background

This article aims to provide a firm understanding of penalty and slashing mechanisms, which are crucial in the Ethereum consensus layer. These mechanisms play a vital role in preserving network integrity and deterring malicious activities. Specifically, we will delve into the details of penalties and slashing and assess their potential implications for Tokemak v2, also considering various scenarios that have occurred in the past.

Penalties and Slashing

In the Ethereum consensus layer, misbehavior is met with two forms of retribution: penalties and slashing. Below, we will explore the distinctions and some details of each of these mechanisms.

Penalties

Ethereum utilizes penalties as a means to address non-malicious technical problems which can be outside of the validator's control and not for possibly malicious attacks on the network.

Validators are required to submit correct and timely attestations (containing their view of the target and source checkpoint of the chain) once per epoch (every 32 blocks, which is an equivalent of roughly 6.4 minutes). For example, in Epoch 209418 the target checkpoint was 6,701,407 and (block 17,518,997) and the source checkpoint was6,701,376 (block 17,518,966).

After a delay of 32 slots there starts to be penalties for late but correct attestations.

Missing attestation can happen for reasons both inside and outside the validators control.

Penalties are generally benign and small and are not expected to have a significant impact on the performance of an LST or Tokemak as a participant in the LST space.

"Note that the attester does not have full control over whether it receives rewards or not. An attester may behave perfectly, but if the next block is skipped because the proposer is offline, then it will not receive the correct head block reward. Or if the next proposer happens to be on a minority fork, the attester will again forgo rewards. Or if the next proposer's block is late and gets orphaned — subsequent proposers are supposed to pick up the orphaned attestations, but there can be considerable delays if block space is tight. There are countless failure modes outside the attester's control."

Source: https://eth2book.info/capella/part2/incentives/rewards/

Slashing

Slashing is a more severe punishment that serves as a deterrent against malicious behavior within the Ethereum network and is applied when consensus rule violations occur that could indicate an attack on the network. Validators can be slashed for the below offenses, which are all treated the same:

1. Related to Casper FFG consensus,
2. Making two differing attestations for the same target checkpoint, or
3. Making an attestation whose source and target votes "surround" those in another attestation from the same validator.
4. Related to LMD GHOST consensus,

5. Proposing more than one distinct block at the same height, or
6. Attesting to different head blocks, with the same source and target checkpoints

When a validator is slashed, they lose 1 ETH in an initial penalty and are unable to earn rewards for approximately 36 days. Additionally, a correlation penalty is imposed around day 18, scaling with the number of validators slashed within a timeframe of approximately 18 days on either side of the slashing offense .

Slashing Scenarios and their Impact on Tokemak v2

During an incident on April 3, 2023, Flashbots was exploited, resulting in the drainage of $20M from multiple sandwich bots. In this particular case, a validator intentionally submitted an invalid block, including a bait transaction targeted at the sandwich bots. As a consequence, the validator faced slashing, losing 1 ETH. However, considering the substantial profits gained from exploiting the sandwich bots, which amounted to $20M, the validator deemed the slashing penalty to be a worthwhile trade-off.

External Incentives Make Slashing Profitable

This type of slashing poses a minimal risk to Tokemak for several reasons:

- The slashing incident affected only a single validator.
- The slashed validator was not associated with an LST protocol.
- Large-scale third-party exploits are generally infrequent.
- The primary targets of such exploits are typically not the LST protocols themselves, but rather third parties, such as the sandwich bots that relied on Flashbots' trust.

Considering these factors, the specific slashing incident described does not present a significant risk to Tokemak.

Node Operator Unintentional Technical Mistake

Accidental technical errors by LST node operators have been a primary cause of slashing events. These events typically arise from configuration errors or bugs specific to a single operator, rather than system-wide issues:

- On April 13, 2023 a Lido Node Operator named RockLogic had 11 of their validators slashed This was because of a bug where they accidentally had several nodes with duplicate validators keys.
- On February 2, 2021 Staked had 75 of their validators slashedby accidently signing a single block twice. Because this was earlier in the beacon chain development the initial penalty for slashing was less at .25 ETH so they only lost 18 ETH to the slashing.

Multiple safeguards are implemented to mitigate the occurrence of large-scale accidental slashing incidents resulting from minor bugs. In the aforementioned cases, the slashing of validators was attributed to configuration errors made by a single node operator, rather than a widespread system-wide bug. These safeguards play a crucial role in minimizing the likelihood of such incidents.

LST protocols, along with Ethereum validators in general, strive to foster diversity among node operators and client software. This approach aims to mitigate the potential risk of a bug leading to simultaneous slashing of numerous validators. This is a report on the consensus layer client diversity of Lido in Q1 of 2023.

Occasional accidental technical errors are not anticipated to have a substantial impact on slashing. Moreover, numerous protocols incorporate an additional layer of protection through an "insurance fund." For instance, Lido has established its insurance fund, Rocket rETH, utilizes staked RPL as a form of insurance for each node to safeguard against significant slashing events. These measures provide an added level of security and mitigate the potential consequences of slashing incidents.

These inadvertent minor slashing events do not pose a significant risk to Tokemak due to several factors:

- There is a high level of diversity among node operators, LST protocols, client software, and consensus software. This diversity reduces the likelihood of large-scale slashing events, making them relatively infrequent and limited in scope. Bugs are thus more likely to have a localized impact.
- As of June 21, 2023, a total of260 validators have been slashed, with 242 of those incidents attributed to "Attestation rule offense." When a bug is detected, node operators can promptly and easily pause new attestations. This proactive response was the immediate action taken by both organizations during the significant slashing events mentioned above.

Considering these factors, the accidental occurrence of minor slashing events poses no serious threat to Tokemak's operations and security.

Inactivity Leak

In the event where at least one-third of validators cease to submit attestations, the consensus layer becomes unable to finalize. Consequently, the offline validators will experience a gradual reduction in their balances until the effective balance of the online validators surpasses two-thirds of the total staked ETH.

While it is true that such a scenario would pose a significant risk to Tokemak, it is important to highlight that the conditions necessary for LST protocols to encounter significant slashing resulting from an inability to meet attestation obligations, are exceedingly rare and would arise in extremely severe circumstances (such as global conflicts or comparable catastrophic events).

Coordinated Massive Attack on the Network

The slashing mechanism is designed to impose smaller penalties in cases where it is not perceived as an attack on the network, while imposing more significant penalties in situations where it appears to be part of a coordinated attack. This mechanism incorporates the concept of the "correlation penalty." If a substantial number of validators are slashed within a ~36 day period, they will all receive a heightened penalty that scales based on the proportion of validators slashed during that time frame.

There are a couple of ways in which this can occur. One possibility is if malicious actors gain control over a large LST, another scenario could arise if an unnoticed bug in a consensus layer client, such as Lighthouse, starts causing issues after being adopted by a substantial portion of node operators. These scenarios would pose a significant risk to Tokemak.

Conclusion

Thus far, no slashing events have occurred due to the correlation penalty. The instances of slashing that have taken place were minor and accidental, resulting from configuration errors or unfavorable incentives associated with MEV. Penalties arising from missed attestation votes are also minimal and can be attributed to random issues beyond the validators' control.

Considering the diversity of LSTs, node operators, and software, it is unlikely that a technical error would significantly impact the required number of nodes for a consensus penalty.

The main slashing risk to Tokemak lies in holding an LST controlled by a malicious actor actively engaging in network attacks.

Discord: https://discord.com/invite/tokemak

Website: https://www.tokemak.xyz/

Medium: https://medium.com/tokemak

Twitter: https://twitter.com/tokenreactor