Sei Giga, Under the Hood - Part 3: Economics

Sei Giga will be the new exciting era for the Sei blockchain system.[1] Sei Giga will mark a major shift in how transactions are published, processed, and finalized in Sei. For this reason, Sei Labs commissioned Common Prefix to review the Sei Giga proposal and outline its findings in a series of blog posts.

In the third and final instalment we will discuss the economics of Sei Giga. At the time of writing this article, Sei Giga is expected to follow, for the most part, the economics of the existing Sei deployment. Nonetheless, since game theoretic dynamics play a big role in blockchain systems, a closer look is important to understand Sei in terms of incentives and the expected behavior, or potential hazards, that arise from them.

Reward allocation

In Sei Giga, each block yields a reward. In a more traditional approach, taken in systems like Bitcoin, the reward is given directly to the party that created the block. In Sei though, reward allocation is organized in epochs. During each epoch, the aggregate rewards of all blocks are pooled. Following, these rewards are shared among all validators that participated in the consensus protocol during the epoch. Each participant's reward is proportional to their stake, which comprises both their own and their delegated stake. Of the rewards given to a validator, the participant receives an amount proportional to their own stake, plus a commission, and the rest are distributed to the parties that delegated stake to them.

This distribution approach has been explored before[2] and offers benefits compared to the standard block-based approach. First, some blocks may yield higher rewards due to increased fees of the transactions published in them. This may lead to competitive dynamics between block producers, even resulting in known attacks such as selfish mining.[3] By distributing an entire epoch's rewards across all participants, the variance of mining rewards is reduced, which in turn both avoids some hazards and potentially promotes decentralization.[4]

Additionally, in Sei Giga, rewards are dependent on a node's performance. Specifically, as long as a validator proposes or validates at least some blocks in an epoch, then their performance is considered adequate enough and they receive all rewards. Interestingly, the extent to which a validator's rewards are dependent on performance results in the following tradeoff.

---

[1] https://www.sei.io
[2] For example, Cardano also follows an epoch-based reward distribution approach: https://docs.cardano.org/about-cardano/learn/pledging-rewards
[3] https://arxiv.org/abs/1311.0243
[4] A similar idea can be found in the FruitChains protocol: https://eprint.iacr.org/2016/916

If performance is not closely linked to rewards, then the system risks introducing a free-rider problem.[5] Imagine a case where someone receives full rewards as long as they participate in the creation of 50% of all blocks in an epoch. Here, the party is incentivized to go offline as soon as they meet this target, in order to avoid unnecessary uptime costs. In other words, each party would be incentivized to be active only throughout half the epoch, which would expectedly hurt the overall system's performance and even result in liveness hazards like stalling.

On the other hand, if performance is very closely linked to rewards, then validators would be punished for even small, unintentional downtime. For example, if the allocated rewards are exactly equal to a party's participation rate, then missing a single block, e.g., due to a temporary network outage, would lead to reduced rewards. In turn, this would require very high uptime guarantees which, although useful, can lead to the centralization of validators around cloud hosting services that can offer them.

To make matters worse, the measurement of a validator's performance may be affected by other malicious - or rational - participants. Performance is measured in terms of the blocks that a party proposes and signs. In more detail, the reward allocation mechanism parses each block in the final chain and marks a validator as active if they have proposed and/or signed a block, based on the signatures published in it. However, this set of signatures is controlled by the block's proposer. Briefly,[6] in Sei Giga's consensus protocol, Autobahn, the leader first proposes a block, then collects signatures from other participants, and finally publishes a certificate of at least 2f+1 signed confirmation messages.[7] Crucially, the leader chooses which signatures are included in the certificate. Therefore, by excluding some signatures, a leader may artificially reduce the measured performance of a validator.

For example, imagine that Alice is the consensus leader at some point in time. There exist five participants in total (Alice, Bob, Charlie, David, Eve) and the adversarial threshold f is 1. Alice proposes a block and she receives signatures from all others. However, when crafting the new block's certificate, Alice includes only the signatures from Bob, Charlie, and David and excludes Eve's. The certificate contains signatures from ⅘ parties, so it is valid and becomes finalized. However, when measuring Eve's performance at the end of the epoch, she appears to not have participated in this block's validation, although in reality she did everything correctly and it was Alice's actions that excluded her.

This hazard becomes significant both if rewards are closely linked to performance, as discussed above, and if all rewards are allocated regardless of performance. In the above scenario, if the rewards that Eve misses are redistributed among the other validators, then all other validators directly profit from Alice's actions. Therefore, each validator has a direct incentive to reduce the measured performance of others, in order to increase their own amount of rewards. Even if

---

[5] https://en.wikipedia.org/wiki/Free-rider_problem

[6] See part 1 of our review for more details on Autobahn consensus.

[7] Here f is the assumed adversarial threshold of the protocol. In other words, as long as the malicious parties are less than f, which is typically ⅓ of all participants, then Autobahn consensus is proven to be secure.

Eve's missed rewards were burnt though, instead of being reallocated, other parties could still be incentivized to exclude her, in order to increase their *relative* rewards.

Slashing

Sei Giga follows Sei's model in implementing penalties for participants' misbehavior. These penalties apply to two broad families of violations, against safety or liveness.

In terms of safety violations, Sei Giga slashes parties that sign conflicting messages. If a party signs two consensus blocks that exist at the same height of two forks of the chain, then the party is heavily penalized by forfeiting part (or all) of their stake. The reasoning is that such a penalty disincentivizes parties from creating forks.

In terms of liveness violations, Sei Giga penalizes parties for failing to participate in consensus. In other words, if a party fails to propose a block when they are the designated leader, or if they fail to sign a block created by the leader, then they face potential penalties. Slashing for liveness violations is less severe compared to safety ones, for the reasons discussed in the previous section. However, as we discussed above, a node's performance can be affected both due to temporary outages and, crucially, by the actions of other parties. Therefore, allowing a correct party to get slashed is particularly problematic and should be carefully handled and avoided.

To make matters more interesting, another question relates to how slashed stake is treated. One approach is that the assets are repurposed, e.g., to reward the party that reports a misbehavior or to fund a community pool. Although this approach has the benefit of utilizing these assets, it is complicated and may lead to inadvertent behaviors, if not carefully designed. The alternative approach, which is currently taken by Sei,[8] is to simply burn the slashed tokens. This is a straightforward process and perhaps the best suited choice for most use cases.

Finally, a crucial point regarding the effectiveness of slashing is the amount of each validator's own stake, compared to their delegated stake. In other words, how much "skin in the game" each validator has and how much they stand to lose if they misbehave. This is particularly relevant when considering the maximum number of validators that Sei Giga can support in practice.[9]

For example, say that 200 validators participate in Sei Giga and the security threshold is ⅓ of these validators' total stake. Therefore, if, say, 50 validators control ⅓ of all stake, then they can break the system's security, as Autobahn's guarantees would no longer hold. Crucially, this stake may not be their own, but delegated to them. In that case, these 50 validators may stand to lose much less than their delegators, so their counter-incentive could be much lower than the nominal ⅓ of all stake.

[8] https://www.docs.sei.io/learn/general-staking#slashing
[9] For more details see the scalability discussion in Part 1 of our review.

Interestingly, in Sei's existing deployment, most validators do indeed demonstrate significantly less stake than their delegators. Specifically, the 7 validators that currently control 33% of all stake have self-bonded zero Sei tokens.[10] Therefore, if they decide to break security they stand to lose nothing, besides their good name, while their delegators would face the full penalty.

Exploring how to resolve this consideration in Sei Giga is a challenging but interesting problem. A possible approach could be to require validators to pledge some amount of their own stake, which can then be linked to their rewards and/or overall attractiveness to delegators.[11]

Asset locking

A final consideration is the locking period of staked assets. In Sei, validators and delegates are required to lock their stake for 21 days. During this time the staked tokens earn no rewards and do not participate in the consensus process. Instead, they are locked in case their owner needs to be slashed.

Unfortunately, although the locking period is necessary to some extent, it hurts the system's usability by restricting usage of the locked assets. Therefore, it should be both long enough to achieve its goal, but also not too long. If the period is too short, then a malicious validator might unlock and transfer their assets before the system manages to slash them. On the other hand, if the period is too long, much longer than necessary, then a - possibly large - amount of tokens remains unusable for more time than needed.

Although this consideration is less consequential than the rewards and slashing choices discussed in previous sections, it can still improve the overall system's usability and enhance the users' experience. If the locking period could be reduced from 21 days to fewer, or even to hours, then this could significantly boost the system's potential and appeal.

Conclusion

In this article we explored the economics and incentives of Sei. Although Sei Giga may make some different choices, currently it is expected to follow Sei's model closely. For this reason, we looked into Sei's reward allocation mechanism and the penalties that are implemented via slashing. We discussed tradeoffs that appear when making certain design choices and, importantly, identified potential hazards and ways in which the system's incentives may not align with those of participants. In such cases, rational parties may be driven to behave unexpectedly and problematically. We note that avoiding such pitfalls and balancing these tradeoffs is a delicate process that needs careful consideration and analysis. Therefore, we envision that Sei Giga will take steps in this direction and offer a nuanced and careful game theoretic analysis, which can benefit both itself and the broader distributed ledger ecosystem.

---

[10] https://www.seiscan.app/pacific-1/validators
[11] Such approaches have been considered in the literature, such as: https://arxiv.org/abs/1807.11218