Please refer to the full post for more details.

Although it might not be a trendy topic, I made this post to discuss the security of Optimistic Rollup. Why I've researched this topic is because @vbuterin argued in his article that we need more explicit reasoning to design auditing incentives for Optimistic Rollup:

Auditing incentives - how to maximize the chance that at least one honest node actually will be fully verifying an optimistic rollup so they can publish a fraud proof if something goes wrong? For small-scale rollups (up to a few hundred TPS) this is not a significant issue and one can simply rely on altruism, but for larger-scale rollups more explicit reasoning about this is needed.

This post discusses why we need to consider auditing incentives, and how we can solve this with a game theoretic approach. Due to lack of space I won't write the whole article here; instead I will share the summary of the post. If you are interested after reading TL;DR below and want to know more, I highly recommend reading the full post.

TL;DR

- It is truly important to implement auditing incentives for the long-term security of Optimistic Rollup.
- This already has been discussed with the concept ofVerifier's Dilemma.
- According to verifier's dilemma, since the economic incentive for verification (auditing) is strongly dependent on the sequencer's attack behavior, the less the sequencer attacks, (i.e, the safer the rollup is,) the less the incentive for verification is.
- We cannot solve this issue by increasing the capital requirement (i.e. increasing the deposit) of the stakeholders (verifiers and sequencers), or the number of verifiers.
- There is an argument that the verifier's dilemma in the Optimistic Rollup is just a trivial issue, and there is no need to implement an additional mechanism to deal with it.
- The rationale behind this argument can be summarized into four main reasons: Token holder, DApp builder, Altruist, and Fast withdrawal. But, the only meaningful approach is the fast withdrawal.
- Since intermediaries of fast withdrawal cannot be protected by other honest verifiers due to the special nature of fast withdrawal, they have relatively higher incentives to verify.
- But this does not mean that intermediaries have incentives to perform verification every single time. This also depends on the attack probability.
- If the intermediary has high risk aversion tendencies, he may always perform verification.
- If we want to force verifiers to perform verification, attention challenge could be a good option.
- However, the nature of the attention challenge requires interacting with L1, so expanding the target and the probability of the attention challenge can be a huge burden at the system level.
- Most desirable method is to wisely apply the attention challenge to appropriate targets, tailored to the level of security each rollup wants to achieve.
- There will be a different target level of security for each rollup, and there will be assumptions about the disposition of the participants. If it is not necessary to guarantee high security, or if the proportion of altruist and extremely risk-averse participants is considered to be high enough, it is not necessary to apply additional mechanisms like the attention challenge.

Optimistic Rollup will be launched soon. In the near future, the optimistic rollup will be widely used and adopted massively. As the number and the size of rollups increase, the security issue will become more and more important.