Arbitrum has recently brought up a discussion on Medium aboutDelay Attacks on Rollups. In short, their post raises an important issue that affects all optimistic rollups that are based on interactive verifications, such as Optimism, Arbitrum, Cartesi, Truebit, etc.

In short, although the attack does not compromise the security of the rollups chain, it allows a well funded party to delay its finality by continuously burning collaterals for the duration of the attack.

This news could have been worrisome, since it affects several different protocols. However Delay Attacks are far from an unsurmountable problem.

First of all, Arbitrum itself has announced in their article that they know a solution to the problem. They have announced a new protocol to be published soon, which is already being implemented.

On another front, Cartesi's contributors have also worked to tackle this Delay Attack and they have just published a solution to the issue in this article.

In summary, under Cartesi's proposal, a team of dishonest parties with x

funds can be defeated in a single dispute by an honest player who is willing to deposit log(x)

funds. This makes Delay Attacks impossible and sibling attacks impractical.

References

Delay Attacks on Rollups - Offchain Labs, Medium.

This article digs into the delay attack problem, and discusses how it was handled in various versions of the Arbitrum rollup protocol.

(…)

This is based on a technical breakthrough from the Arbitrum research team that makes all-against-all challenges feasible and efficient. This allows a single honest staker to efficiently defeat an army of attackers who have posted a forest of malicious branching assertions.

NT - Nehab and Teixeira, ArXiv.

In this paper, we propose a practical dispute resolution algorithm by which a single honest competitor can win disputes while spending effort linear on the cost of the computation, but only logarithmic on the number of dishonest competitors. This algorithm is a novel, stronger primitive for building permissionless fraud-proof protocols, which doesn't rely on complex economic incentives to be enforced.