We study economic security of optimistic rollups, in the paper we put out online recently:

2308.02880.pdf (arxiv.org)

We first argue that any system in which (malicious) asserter and (honest but lazy/rational) validators play a (negative) constant-sum game does not have a pure Nash equilibrium solution, and therefore, full security is not guaranteed. However, the probability of the protocol failure in the mixed Nash equilibrium solution can be lowered arbitrarity, by using few forces in place:

- lowering the cost of checking.
- increasing assertion deposit.
- increasing validator deposit.
- increasing total value locked.

The main (mathematical) result of the paper is that the probability of the system failure in mixed Nash equilibrium solution increases in the number of (staked) validators, as they compete for the share of malicious asserter's deposit. The result is not trivial, since even if individual level of checking is decreasing with more validators, there are more of them independently trying.

To the end, we argue that pure Nash equilibrium solution, and hence, full security can be guaranteed by introducing system-wide rewards and derive optimal levels for it.