We described a crypto-economic attack on Validium—added to the post “zkRollup vs Validium”:

Medium – 8 Jun 20

zkRollup vs. Validium (StarkEx)

StarkEx is a major security enhancement for exchanges—but its operators can still freeze and seize your funds.

Reading time: 7 min read

@JustinDrake pointed out that data availability approach of Validium can lead to an unexpected attack vector: should the signing keys of the quorum of the Data Availability Committee be compromised (and these keys are kept online, which makes it notoriously hard to secure them), attacker can transition Validium into a state only known to them, thus freezing all assets, and then demand ransom to unlock it.

Theoretically, the contract upgrade mechanism should mitigate this attack. Validium’s operators could initiate deployment of a new version where the state is reverted to the last known one after 28 days of upgrade notice period. It would be a month of locked capital (which of course has quite significant costs), but if the DAC refused to negotiate, attacker would not get a single penny.

However, it turns out there is a way for attacker to force the operators into deciding between losing everything or allowing the attacker to make a double-spend. It can be illustrated with the following example:

Imagine that you can hack an ATM in such a way as to erase the entire bank database after your withdrawal is complete. You can only withdraw from your own account, but the details of the operation will be lost when the DB is gone.

Bank employees can go through a complicated process of restoring the database in one month. But since they don’t know who did the withdrawal, by reverting to the last checkpoint they will also restore the balance on your account that you have withdrawn!

Of course, this double-spend will be limited to the amount the attacker can provision on their account. However, it is trivial to construct a trustless contract and borrow the necessary capital from evil anonymous whales in the darknet.

This attack demonstrates that the security model of Validium is relatively similar to that of a PoA network. In fact, a PoA network with 20 nodes and 51% signing threshold might be more secure

than a Validium with 8 nodes and 100% signing threshold.