Risk Management Case Study: Agora / Metis

Gauntlet

Follow

Gauntlet

--

Listen

Share

While many users are familiar with the risk of liquidations and insolvencies in DeFi, there are also latent risks that are less visible to most participants. The risk of contagion between various DeFi protocols may seem abstract, but can have very real consequences for the protocols involved and even an entire DeFi ecosystem.

This case study reviews the early history of the Metis ecosystem, which was significantly disrupted by a multi-protocol exploit in April 2022. Though the initial catalyst was a smart contract bug, a number of economic weaknesses compounded the damage to Metis' overall competitiveness.

Background

Metis is an Ethereum Layer 2 (L2) network that launched in late-2021, competing with similar networks like Optimism. At the time of the events, the top lending protocol on the Metis network was Agora, a fork of the popular Compound V2 design. Starstream was a yield aggregation protocol on Metis that had grown quickly in the ecosystem's early days. The Starstream governance token (STARS) was listed on Agora, where it could be used as collateral for loans.

Events

On April 7, 2022, a poorly configured Starstream treasury contract was drained of a large quantity of STARS tokens. In a single transaction, the exploiter was able to gain control of over 50% of the total supply of STARS, worth about $10M at the prevailing market prices. The drained tokens were then supplied to Agora, where they were used to execute a price manipulation attack.

The exploiter used STARS collateral on Agora to open an initial borrow position. A portion of the borrowed assets was then used to buy STARS on the Tethys DEX, which provided the sole price feed for STARS collateral on Agora. As the price of STARS temporarily spiked, so did the exploiter's borrowing power, allowing them to further increase their borrow position on Agora. The borrowed tokens were eventually moved to other addresses, resulting in about $8.4M worth of bad debt on Agora. Within a few weeks, both Starstream and Agora had shut down, leaving the Metis ecosystem without a core lending protocol. The contagion disrupted DeFi activity across the Metis network and was a major setback in its growth trajectory.

Analysis

The Starstream/Agora exploit highlighted several vulnerabilities across both smart contract and economic risk. Though better smart contract audits may have caught the initial treasury vulnerability, this was only directly relevant to Starstream. The later fallout for Agora and the entire Metis ecosystem was not a result of smart contract bugs, but rather economic weaknesses:

- Agora listed STARS as collateral without any supply limits, since Compound V2 forks do not have the native ability to do so. Though Agora planned on adding supply limits in a later upgrade, this had not yet been implemented at the time of the exploit.
- The initial 40% collateral ratio for STARS was aggressive given the risk profile of the token and lack of supply limits. Agora was preparing to lower the collateral factor from 40% to 20% at the time of the exploit, but this change had also not yet been implemented.
- The STARS price oracle on Agora was based on a 1 hour TWAP of a single trading pair on the Tethys DEX. A relatively small DEX pool is far more vulnerable to manipulation than advanced oracles using multiple price sources or sophisticated filters for price data.
- Agora did not have automated systems in place to detect unusual activity, such as an outsized supply position.
- Metis relied heavily on Agora as its top lending protocol, making the loss very damaging to the ecosystem.

Addressing these economic issues could have helped contain the fallout from the Starstream events. In a robust ecosystem, overall DeFi activity can continue relatively unaffected after a localized exploit. Since it is likely impossible to prevent all hacks and exploits entirely, reducing contagion is a key consideration for the long-term success of an emerging ecosystem.

Conclusion

This case study highlights the latent nature of economic risk and its links to other risks across DeFi ecosystems. Though the draining of Starstream's treasury was the immediate catalyst, it revealed economic issues in the Agora and Metis ecosystems that were always present in the background. A better code audit may have prevented the initial Starstream exploit, but the economic issues would have remained. Unless remedied, the ecosystem would always be vulnerable to market shocks or exploits that would have eventually exposed these weaknesses.