A game-theoretical analysis of potential AVAX-USD price manipulation attack on AAVE

This is Theo from the Risk DAO, a service DAO launched by B.Protocol and 1kx research arm (not associated with the risk dao initiative of Aave).

A recent manipulation of the AVAX-USD price pair resulted in significant losses for liquidity providers on GMX, a perpetual swap DEX on Arbitrum.

In this post, we'll examine what happened and how this attack vector can be replayed on the Aave protocol. Whilst also relevant to other lending protocols the sheer size of Aave's borrow markets represent an attractive target as even small percentage gains could mean substantial USD profits for the attacker.

TL;DR:

- The attack scenario looks like the following: An attacker can artificially inflate the AVAX price, deposit the token into Aave and borrow against this inflated collateral value. A similar attack played out for the Venus Protocol in May 2021 which bankrupted the protocol.
- Liquidity and LTV are the key profitability drivers: Lower exchange liquidity allows the attacker to manipulate the price much easier (i.e. less cost required), whilst a higher LTV on Aave allows more borrow power (i.e. higher cash proceeds).
- We show how different liquidity curves may make price manipulation profitable. We look at super-linear, linear and sublinear slippage functions.
- We conclude that in this simplistic framework the attack is not profitable, however further research is needed, and risk managers of lending protocols need to closely monitor slippage levels of collateral tokens and associated LTVs to pre-empt malicious attacks.

AVAX-USD exploit on GMX - What happened

On 18 September, a trader engaged in a series of trades to impact the price of AVAX by >2%. This does not seem substantial at first sight but cost Liquidity Providers on perpetual swap exchange GMX.io dearly, losing approx $0.5m. GMX offers zero-slippage trading, based on oracle prices fetched from CEXes.

The trader successfully extracted profits from GMX's AVAX-USD market by opening large positions at 0 slippage, then moving AVAX-USD on CEXes in their favor. The trader switched from long to short 5 times over an hour, creating a sinusoidal pattern.

Notional trade sizes ranged between $4.2m to $4.8m.

twitter.com

Joshua Lim

@joshua_j_lim

3/ let's take a look at the first cycle which took place from 01:15:31 to 01:28:11 UTC. X was able to extract roughly $158k in profit by trading clips of $4-5mm at a time https://t.co/W6eu7Iz6lz

5:38 PM - 18 Sep 2022 87

5

Some trading sleuths on CryptoTwitter put the price of the attack at c. $700k, mostly from slippage on the CEXes.

twitter.com

alphanonce Intern

@alphanonceStaff

How about slippage? The trader made a 2.2% [$18.3-$18.7] price impact. If half of the price impact was slippage, 1.1% would be the cost that the trader paid

70M x 1.1% = 770K

402K - 770K = -368K

If the above assumption is true, then the exploiter lost money in the trade

7:08 AM - 22 Sep 2022 8

The choice of trading venue (GMX) and time (low volume weekend hours) is not by chance and enabled the incident.

Connecting the dots - How can such an attack vector be replayed on Aave?

Aave markets also fetch prices from Chainlink Oracles and thus rely on external data to quantify borrow limits and liquidation data.

Price manipulation can be a substantial threat to the stability of the Aave protocol: By artificially inflating asset prices, a trader can deposit overvalued tokens and drain borrow assets from the protocol.

In terms of profit, the attacker would walk away with whatever borrowing proceeds he can generate less the cost of the collateral asset (which gets deposited).

A similar attack played out in a major exploit in May 2021 with $VXS, Venus Protocol's governance token, at the center of it. Whales bought a significant amount of $VXS token and deposited them as collateral on Venus Protocol at the peak, bankrupting the protocol in the process (as can be tracked on the Bad Debt Dashboard the Risk DAO has published).

What are the costs involved?

First up, let's look at the required bankroll: The trader needs to acquire AVAX as collateral asset and move the price in the process.

By looking at the GMX incident, some estimates suggest a $700k price tag, based on slippage and the aggregate trading volume. It is not clear what the attacker's bankroll was but aggregate trading volume amounted to $70m over the period of the attack. However, this was a series of trades where the attacker went long and short and thus could recycle the bankroll.

As referenced earlier, a series of trades in the mid-$4m range (notional size) were entered which moved the price by approx 2%. Looking at the AVAX-USDT pair on Binance, it would cost approx $1.3m for a 2% move on a normal weekday.

Modeling methodologies for the price curves

Let's imagine Trader Alice who wants to manipulate the AVAX price by 100%. Her preferred trading venue is Binance and she assumes that every $1.3m trade moves the price by 2%.

We define the following variables:

slippate_rate: Assumes 2% for every trade of $1.3m

qty_trade: This is the n-th trade.

price_current: AVAX-USD price of $17.5 (as of 28 September 2022)

price_target = price_current*2

The following slippage functions are modeled:

Super-linear case:

Price_new = price_current * (1+slippage_rate)^qty_trade

Assumes that slippage would increase the higher the percentage change is compared to price_current. This could be explained by positive reflexivity and more traders going long whilst supply of the token remains static.

Linear case:

price_new = price_current * (1+slippage_rate*qty_trade)

Assumes slippage stays constant regardless of the price changes.

Sublinear case:

price_new = price_current * (1+slippage_rate*qty_trade^0.9)

Assumes the slippage rate decays as token price goes up. A rising token price would attract traders who sell their tokens into the price rally thereby suppressing the slope of the price curve.

The cumulative growth rates for the three slippage functions is visualized in the table below (for the first 10 trades).

Modelling results

Super-linear function

Assuming an super-linear increase of the price based on 2% slippage, Alice would spend $45.5m to acquire 1.9m $AVAX at an average price of $24.5.

In terms of profitability, this trade would generate a loss of $3.3m. “Value” is defined as the post-pump price of $35 multliplied by the number of $AVAX token acquired.

Linear function

If the 2% slippage persists in a linear style, Alice would spend $65m to acquire 2.6m $AVAX at an average cost of $25.4.

In terms of profitability, this trade would generate a loss of $6.8m.

Sub-linear function

Assuming a sublinear function so that the slippage rate decays by a factor of 0.9, Alice would spend $100.1m to acquire 3.9m $AVAX at an average price of $25.8.

In terms of profitability, this trade would generate a loss of $12.1m.

Conclusion

Given the current risk parameters, the probability of a replay of the GMX attack on Aave is unlikely: The trade is just not profitable enough and an attacker would need to deploy significant sums in this high-risk strategy.

The scenario with a steeper slippage function (ie super-linear scenario) is more advantageous for malicious actors, as evidenced in the below summary chart: It costs the attacker less to pump the price. Albeit in our model it would still not result in a profit.

In the case of higher LTVs, however, this strategy could turn profitable giving malicious actors an incentive to attack.

Thus, risk managers need to watch the token order books for slippage and LTV parameters to stay on top of a potential gamification of collateral prices.