There have been many discussions about oracle and market manipulation throughout the Aave forum and community. These two terms are often used interchangeably, but defining and differentiating them is essential.

To help clarify the difference between market manipulation and oracle exploits, we've recentlypublished a blog that explores these two attack vectors, how Chainlink Price Feeds are designed to report the market-wide price of assets, and ways to increase the security of applications like Aave.

Below is an overview of the article and core concepts to understand. However, we encourage you to read thefull article for a complete understanding of the manipulation methods, risks, and mitigations.

Market Manipulation vs. Oracle Exploits

What Is Market Manipulation?

Market manipulation is when the price of an asset is artificially manipulated through the alteration of natural supply and demand forces. It's a deliberate action undertaken by a malicious actor, usually at the expense of other traders.

The ability of a malicious actor to manipulate prices depends on the liquidity of an asset. The lower the liquidity, the less expensive and difficult it is to manipulate a given market. The liquidity of an asset depends on its trading volume, market depth, and trading markets.

Risks of Market Manipulation

While the price oracle used by a DeFi protocol to receive financial market data may be operating without issue, protocols can still be at risk if the underlying markets on which the oracle reports are manipulated. Lending protocols like Aave can accrue toxic debt and even become insolvent if they don't liquidate undercollateralized positions in a timely and efficient manner. Users' funds can also be unfairly liquidated based on artificial price changes, resulting in losses.

What is an Oracle Exploit and the associated risks?

Oracles deliver external data such as digital asset prices, the outcomes of sports matches, and weather information to blockchains and smart contracts. An oracle exploit occurs when an oracle reports inaccurate data about an event or state of the external world. This can happen because the oracle purposefully acts maliciously or negligently, or the oracle's data source is compromised.

The negative consequences of oracle exploits for DeFi protocols such as money markets include depegged stablecoins, malicious arbitrage trades, unwarranted liquidations, and protocol insolvency. While the risks of oracle exploits are similar to those of market manipulation, they stem from a different root cause.

This is because both market manipulation and oracle exploit attacks leverage artificial changes in price data that diverge from the natural supply and demand forces of the market. So while the risks may be similar, the mechanisms that make them possible differ.

Highly Secure Oracles

The risk of oracle exploits can be mitigated with more secure oracle design. Features of secure oracles include sourcing price data from across all trading environments to provide proper market-wide coverage, protections from external tampering that eliminate single points of failure via decentralization, and economic incentives to report faithfully that align oracles with their users.

What Is the Fundamental Difference Between Market Manipulation and Oracle Attacks?

Market manipulation changes the price of an asset, while oracle attacks result in incorrect or invalid data being reported that doesn't reflect true asset pricing. Because the end result is an asset price that leads to a loss of funds, these issues have historically been confused and conflated.

Properly designed oracles accurately report prices based on the actual market-wide price of an asset, regardless of the level of healthy liquidity in the asset's underlying markets. If the market-wide price of an asset has been manipulated, the oracle will still report that price—it's what oracles are designed to do. What's different about oracle attacks is that the market price can still be based on real supply and demand pressure. Instead, the oracle reports false information through either unintentional or malicious behavior.

[

Market Manipulation vs Oracle Exploit Example

1928×488 49.2 KB

](https://europe1.discourse-cdn.com/business20/uploads/aave/original/2X/9/92e78158f9deed3aab0d0dc77f2c97cc38f4c480.png)

As the above table highlights, the point of failure for market manipulation and oracle attacks is different. To build a secure DeFi protocol that protects users from market manipulation and oracle attacks, developers must consider the security properties of both the oracle they use as well as the quality of an asset's underlying market, including its market volume, depth, and trading environments. If these considerations are not taken into account, then a protocol may be designed in a way that does not properly mitigate risk.

Chainlink Price Feeds Protect dApps From Oracle Exploits

In order to mitigate the risk of oracle exploits, applications can integrate Chainlink Price Feeds to access high-quality, tamper-proof market data.

Chainlink Price Feeds have a range of security features, including multiple levels of decentralization, hyper-reliable oracle node operators, and a defense-in-depth approach through a multi-layered design.

[

chainlink-protects-against-oracle-exploits

1536×864 112 KB

](https://europe1.discourse-cdn.com/business20/uploads/aave/original/2X/a/a3a410655ff20a9209b0d94bb5a5792475d97721.jpeg)

Chainlink Price Feeds in the Presence of Market Manipulation

If the market-wide price of an asset is manipulated, Price Feeds will report that price because it accurately reflects the current state of the market—the accurate truth. But if only a small subset of an asset's underlying market is manipulated (e.g. a few low-liquidity markets), then Chainlink Price Feeds are designed to still report the accurate overall market-wide price, helping protect from such manipulation attempts.

Along with Chainlink Price Feeds' multiple layers of aggregation, the use of volume-weighted average price (VWAP) methodology (plus similar methodologies) and outlier detection plays a key role in preventing market manipulation within subsections of the overall market from influencing reported asset prices. VWAP mechanisms place more emphasis on where more trading activity takes place and seamlessly adapt as liquidity moves across various markets, while data aggregators commonly filter out market anomalies like flash crashes, wash trading, and other outliers so they don't influence the final aggregated data point.

How DeFi Developers Can Protect Their dApps

The first step for DeFi developers who need to protect their dApps is to integrate Chainlink Price Feeds for highly accurate, tamper-proof, and hyper-reliable price data. Next, developers must consider the quality of the assets their protocol supports. Thinly traded assets can make protocols vulnerable to exploits when used as collateral, as they're easier for malicious actors to manipulate. Additionally, consider further layers of security in your dApp, such as circuit breakers, contract update delays, manual kill switches, and active monitoring.

Conclusion

We hope this clears up some confusion on oracle vs. market manipulation to help the Aave community correctly understand and evaluate the risks of each. To dive deeper into these concepts, you can read the full blog here.

Ultimately, securing assets across Web3 requires a multifaceted approach, and we must all work together to ensure users' funds remain safe and secure.