**Blog: Understanding Price Oracle Manipulation**

DeFi strives to revolutionize financial services, one of the main risks facing DeFi is cyberattacks stealing investor's funds from platforms. The [most common](https://coingeek.com/the-defi-hacks-of-2020/) DeFi hack is oracle manipulation, a partial list of platforms that fell victim to this attack are [yEarn](https://blog.trailofbits.com/2020/08/05/accidentally-stepping-on-a-defi-lego/), [Harvest](https://www.rekt.news/harvest-finance-rekt/), [xToken](https://www.rekt.news/xtoken-rekt/), [bZx](https://peckshield.medium.com/bzx-hack-ii-full-disclosure-with-detailed-profit-analysis-8126eecc1360), [Cheese Bank](https://peckshield.medium.com/cheese-bank-incident-root-cause-analysis-d076bf87a1e7), Synthetix.

Smart contracts are great at executing predetermined code but their main weakness is that they are isolated from the outside world and are only exposed to on-chain information.Developers use oracles to solve this problem, oracles are protocols that transmit information from outside the blockchain and add it on-chain so smart contracts are updated. Uploading information on-chain is essential for creating decentralized platforms with real-world use cases. For example, lending platforms need up-to-date asset prices to know if a borrower is under-collateralized and needs to be liquidated (for more information on DeFi lending platforms see [part 2](https://redefine.net/defi-101-part-2/) of the DeFi 101 series). Other use cases include the Augur platform that allows users to bet on the outcomes of real-world activities - like the election results, oracles can upload the results to the smart contract which will settle according to the results.

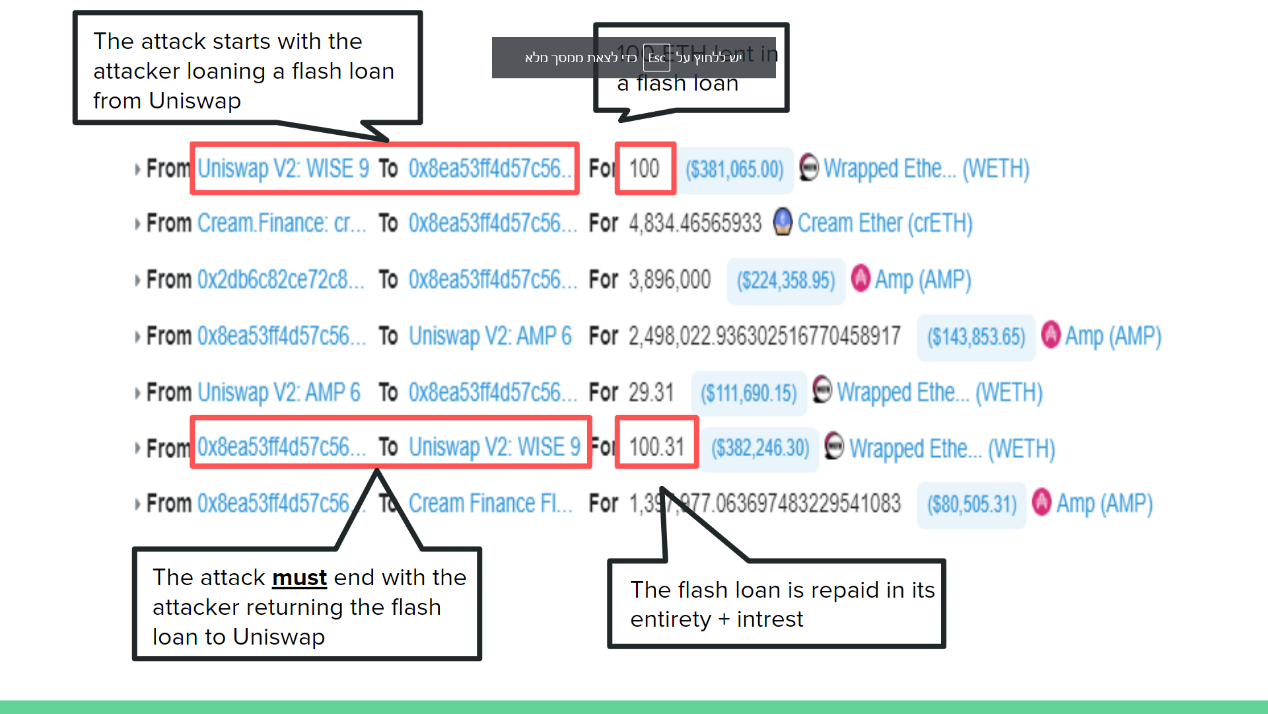
The main challenge with oracles is ensuring that they are sufficiently decentralized to prevent malicious actors from uploading false information. To achieve a satisfactory level of decentralization projects like Chain Link and Band use an incentive structure that incentivizes participants to upload true information and penalizes them for supplying false information. Some projects namely [Maker](https://makerdao.com/en/) put an emphasis on oracle decentralization and aggregate many different price feeds, some of them on-chain and some from off-chain CEX (Centralized Exchanges) and then takes the average between them, price feeds that deviate more than 1% are discarded. This makes an oracle attack on the platform extremely difficult (for more information regarding the [Maker oracle](https://docs.makerdao.com/smart-contract-modules/oracle-module)).

Some DeFi projects don't put as much emphasis on decentralization and rely instead on on-chain information from a single DEX to get a price feed (see [part 2](https://redefine.net/defi-101-part-2/) for more information on DEX). A common method attackers use is to manipulate the price of an asset listed on a DEX using a flash-loan to artificially change its price.

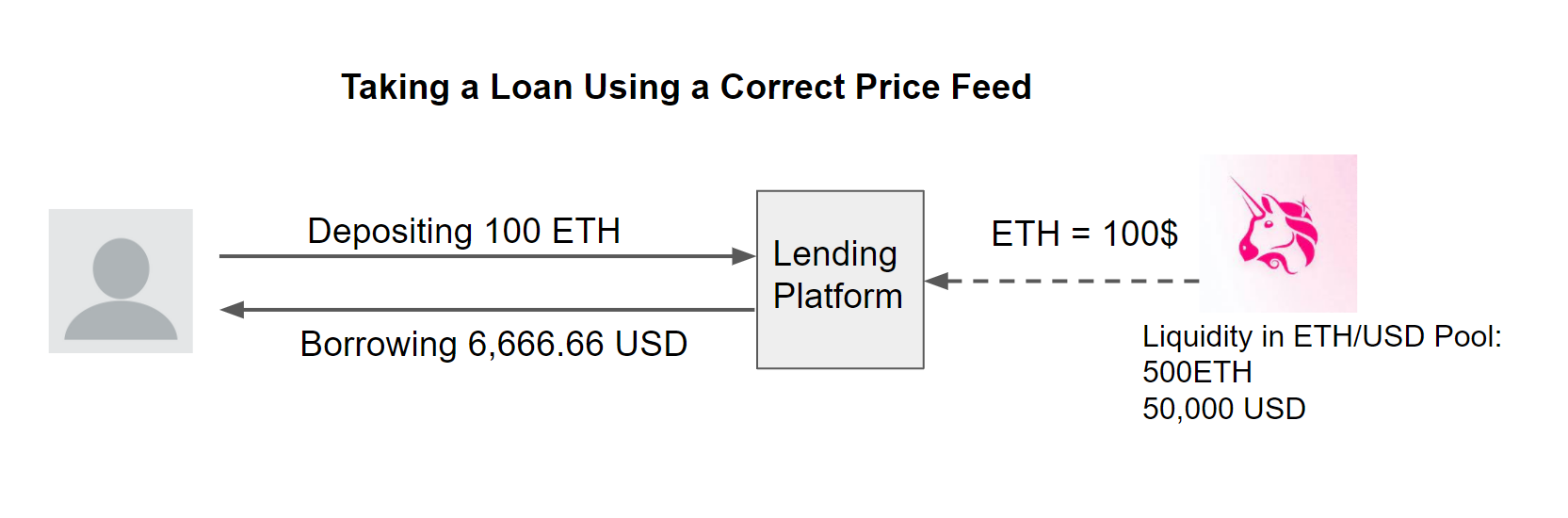
**What is a Flash Loan?**

Flash loan is a financial instrument unique to crypto enabled by the use of smart contracts. Flash loans allow borrowers to loan huge sums of money -virtually an unlimited amount- without collateral for the duration of one block. The flash loan supplier requires the borrower to return the loan inside the same block, if the borrower fails to do this then the transaction reverts and the money returns to the borrower - hence flash loans are risk-free for the lender. Flash loans are beneficial when arbitraging thus have an important part in improving DeFi’s price efficiency. On the flip side, flash loans can also be used by hackers to exploit weakness and inflect huge financial damages in a short time frame. (for more [information](https://decrypt.co/resources/what-are-flash-loans-the-defi-lending-phenomenon-explained)).

Here is an example of a flash loan attack on the CREAM protocol:



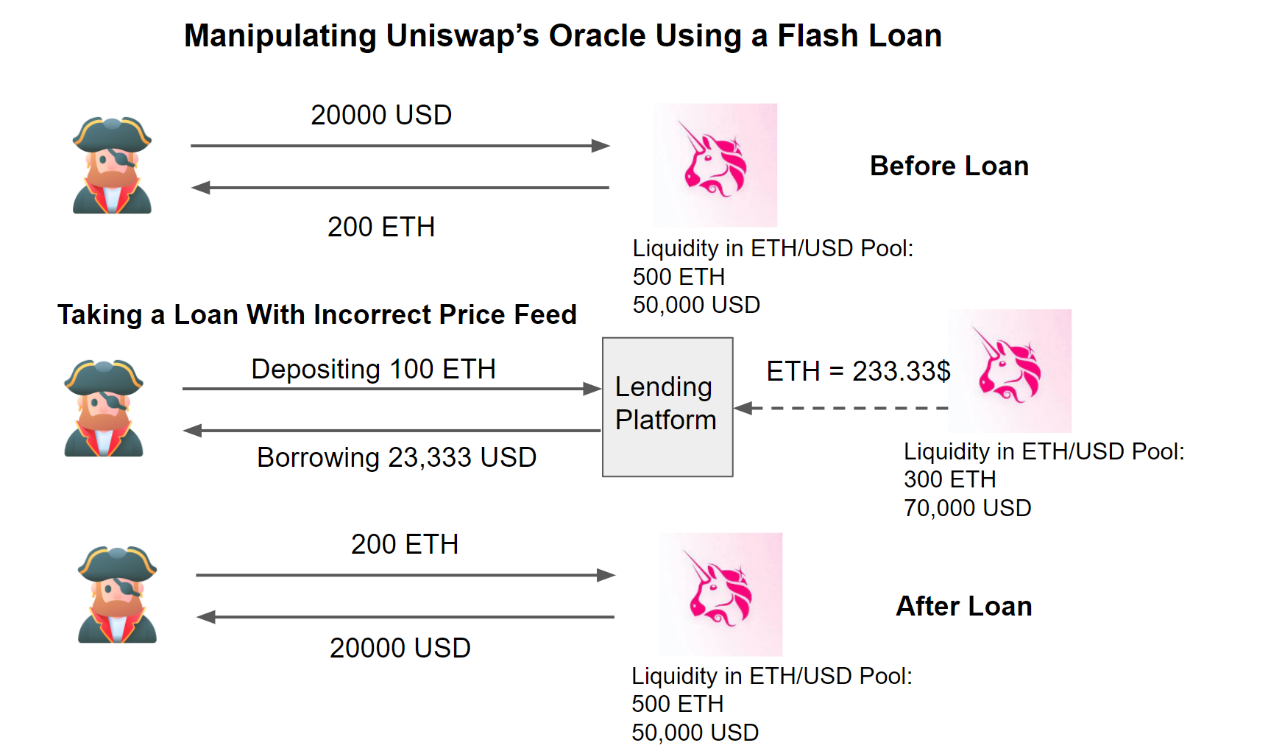
**Oracle Manipulation and Profiting**

Let's assume that an attacker wants to steal funds from a lending platform relying on the Uniswap oracle. The lending platform requires borrowers to have a collateralization ratio of 150%, which means that for every 1$ loaned there needs to be 1.5$ locked on the platform as collateral. For example, a user that deposits 100 ETH as collateral can loan up to 6,666 USD.

**A example for a price oracle attack:**

The attacker loans 20,000 USD using a flash loan. He then trades those 20,000 USD for 200 ETH on a Uniswap ETH/USD pool - assuming 100$ per ETH.

The Uniswap exchange now calculates the price of ETH to be 233.33$. Where previously a user depositing 100 ETH could borrow 6,666.66 USD, now that the price oracle is distorted the same 100 ETH can borrow 15,555 USD.



**Prevention**

The best way platforms can prevent being exploited by this attack is by using the service of a robust decentralized oracle (i.e. Chainlink) or aggregating many different price feeds. If a platform chooses to use the easier to use on-chain oracles, then there are a few precautionary measures they can take to improve platfrom security. Using oracles that are based on pools with deep liquidity that a attacker will be hard pressed to skew the prices enough for it to be worthwhile. Another measure is due to flash loan attacks depending on the attack being completed within the same block, even a small delay in the steps required to interact with the platform can prevent such attacks. This preemptive measure limits composability and user-experience but whenever possible can be effective.

**Conclusion**

Price oracles manipulation is the most common attack method in DeFi today, this is mainly due to its simplicity and because there is almost no cost involved. If they fail, only the transaction fees must be paid, and if they succeed, then the turnover is priceless. Some today are blaming flash-loans and are calling for platforms to stop supplying them. Personally, I believe that these attacks have a cleansing effect requiring developers to strive for even more security and puts an emphasis on decentralization.