Exploring some Attacks on DeFi smart contracts and some Defences

Alireza Darvishi

Supervisor: Prof Qiang Tang

A report submitted in fulfilment of
the requirements of the
Winter vacation program

School of Computer Science
The University of Sydney
Australia

18 October 2021

Abstract

Flash loans, a new way of obtaining funds other than using credit or collateral as in classic finance, have complicated applications. It can be used harmlessly in an arbitrage-taking transaction or a liquidation process that is indispensable, or it can be used as leverage or funds needed to practice a malicious activity or exploit a DeFi and pull money out of it. These kinds of attacks have happened a lot in the last year, which is the main focus of this report.

We will show the idea behind some of the former attacks and propose an attack on a specific kind of DeFi. Then we will suggest some kind of defenses to prevent those attacks, although those are not complete and might have defects. Defenses are focused on preventing attacks using a flash loan, but they won't be effective if the attacker owns the needed funds or obtains them in one way or another.

Contents

List of Figures

CHAPTER 1

Introduction

With the invention of blockchain technology, people could transfer funds without relying on a central authority like a bank [12]. Of course, this trust-less system would cost more for a user because of the transaction fees for the miners who verify and add new transactions to a blockchain. Later on, more complicated transactions were introduced in the Ethereum blockchain [4], called a smart contract.

A smart contract is a predefined code deployed on a blockchain that any user or other smart contract can call and interact with it in a non-custodial, permission-less, and openly auditable way. Some smart contracts called DeFi (decentralized finance) can work as known entities in classic finance, like an exchange, a bank(lending market), a derivative market, an asset management company, or even a money laundry firm [16].

Decentralized exchanges (DEXs) enable users to exchange their assets while they have control over their assets all the time. Moreover, DEXs can be used as a price oracle for other DeFi platforms. Some DEXs work like a classic market with an order book, and others take the risk of price changes and work as an AMM (Automated Market maker)[3]. AMMs are usually more popular due to lower transaction fees. Uniswap [2], dYdX, Curve, and Sushiswap are some of those AMMs.

Some DeFi enable users to lend and borrow assets[17]. Lenders earn interest on their assets which is obtained from interest borrowers pay. Because of the lack of credit defined in classic finance, lending markets provide over-collateralized loans to incentivize borrowers to pay back their debt. By declining the value of collateral relative to a user's liability, their loan is liquidated, and a user called a liquidator would settle the debt and receive the collateral at a discounted price.

Flash loan as an alternative is an unprecedented invention of smart contracts and is feasible due to the atomicity property of the blockchain [15]. The idea lets anyone borrow assets without collateral as long as they return funds and the premium within the same sequence of transactions or otherwise, the whole set of transactions are reverted, and no funds are borrowed at the first step. This kind of anonymous loan is used as capital for many tasks like arbitrage taking between DEXs, wash trading, collateral swapping, and some attacks [5], which is the main topic of this report. In essence, flash loans mean anyone can access an almost unlimited amount of money to do whatever they want with, as long as it can be done fast, on-chain, and without losing the money.

In this report, we are going to discuss a few flash loan attacks on the DeFi ecosystem. Then we will propose an attack on a lending market protocol. Furthermore, we will provide a few defenses for the proposed attack and examine the shortcomings of these defenses.

CHAPTER 2

Some Attacks

In the past few years, there have happened lots of attacks in the DeFi ecosystem, and some of them involved acquiring an amount of capital using a flash loan[13, 9, 14]. Flash loan, in particular, enables anyone to practice those kinds of attacks which needs lots of funds. As there is no default risk, a hacker can borrow the entire pool of funds at any point in time and utilize it to make excess funds and give back the loan and premium. This part is focused on explaining two examples requiring a considerable amount of resources that can be acquired with a flash loan.

2.1 Former attacks

There have been so many DeFi project breaches in the past years to the point that million-dollar hacks don't make the news anymore. Some of those hacks were possible using price oracle manipulation. DeFi protocols need price feeds to function properly. The main idea of these hacks is to mislead the price feed and exploit a victim DeFi in that way.

2.1.1 Harvest Attack

On the 26th of October of 2020, a hacker exploited Harvest protocol [10] and earned $26.6M in total [8]. Harvest Finance is a DeFi yield aggregator. The idea is that users deposit funds into it, and it automatically pools and invests those funds in various strategies that utilize other elements of the DeFi ecosystem. It is a semi-automated hedge fund that uses the power of other DeFi protocols to deliver significant returns, equivalent to around 20-50% APY.

This attack focused on USDT and USDC, stablecoins that used the same strategy when deposited into Harvest. Specifically, USDC and USDT pool automatically earned returns from farming on Curve Finance as liquidity providers. The Curve is a liquidity pool designed for exchanging stablecoins. Users can swap between stablecoins with relatively low fees and slippage on Curve or gain returns on their stablecoins by providing liquidity, which Harvest's depositors were doing.

Generally, revenues from a yield-bearing DeFi application are paid based on the proportion of shares each user holds. However, everyone's proportional share of the pool changes after each withdrawal and deposit, and how it changes depends on the live prices. So Harvest needs to monitor prices whenever someone makes a deposit or withdrawal to calculate how much of a share someone gets when they enter a pool and how many shares they redeem when they leave the pool. Harvest's developers used Curve as the price oracle, and this choice made Harvest vulnerable to the oracle price manipulation.

The idea behind the attack is pretty straightforward. The attacker has to drive up the prices of the deposited asset before the deposit to get more shares. Then he would bring prices back to normal to get more when he redeems his shares. Here is a simple example:

-Assume 1 USDT = 1 share pool

-Boost USDT price up until 1 USDT = 1.1 pool share.

-Deposit 100 USDT and receive 110 pool shares.

-Bring back prices to 1 USDT = 1 pool share. Withdraw 110 USDT and enjoy the 10 USDT as surplus.

Figure 2.1 shows a sketch of the attack which the attacker practiced 32 times.

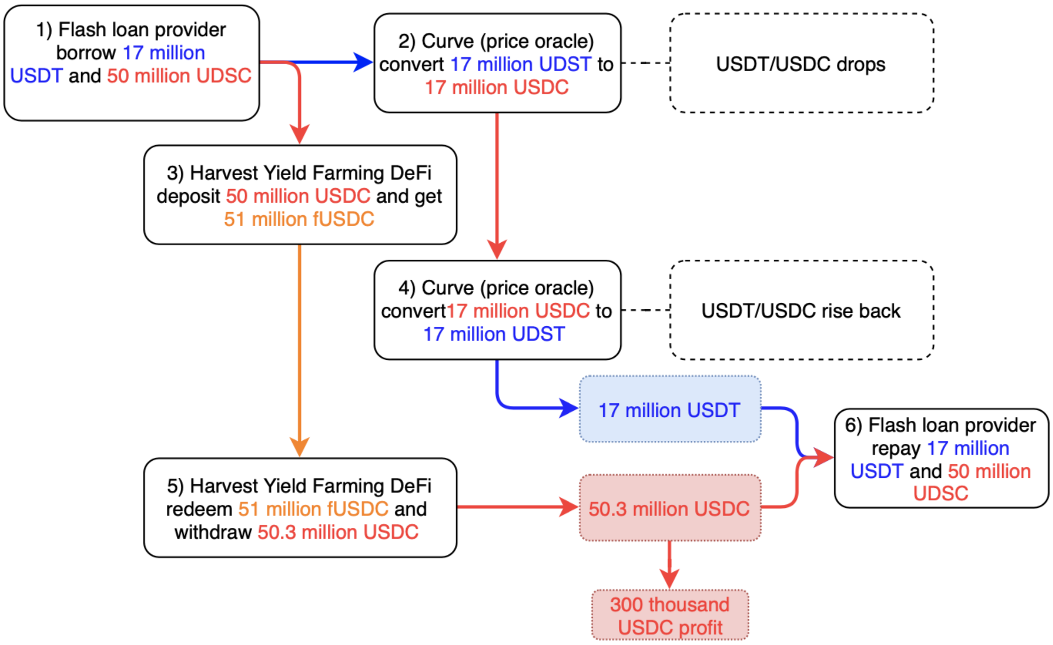
1) Flash loan provider borrow 17 million USDT and 50 million UDSC
2) Curve (price oracle) convert 17 million UDST to 17 million USDC
USDT/USDC drops
3) Harvest Yield Farming DeFi deposit 50 million USDC and get 51 million fUSDC
4) Curve (price oracle) convert17 million USDC to 17 million UDST
USDT/USDC rise back
17 million USDT
6) Flash loan provider repay 17 million USDT and 50 million UDSC
5) Harvest Yield Farming DeFi redeem 51 million fUSDC and withdraw 50.3 million USDC
50.3 million USDC
300 thousand USDC profit

FIGURE 2.1: Price manipulation attack on Harvest DeFi

2.2 Lending market Attack

Lending markets in the DeFi ecosystem are designed to let users gain interests by depositing assets and using deposited funds as collateral to borrow other assets. A borrower must provide collateral proportional to his debt with a predefined factor of more than 1. To ensure that enough collateral supports the loan, liquidators can buy the collateral at a discounted price and pay back the unhealthy loans with insufficient collateral. The lending market itself needs to know the prices to let liquidators take their part, and it must get price feeds from a price oracle.

A scheme to exploit a lending market is to manipulate the price oracle such that some loans become prone to liquidation. Then make use of those loans and buy assets at a discounted price. Assuming the lending market uses an AMM as a price oracle, the attacker can use flash loans and gain more with less risk. Figure 2.2 shows a sketch of the attack on a loan of ETH with USDT as the collateral.

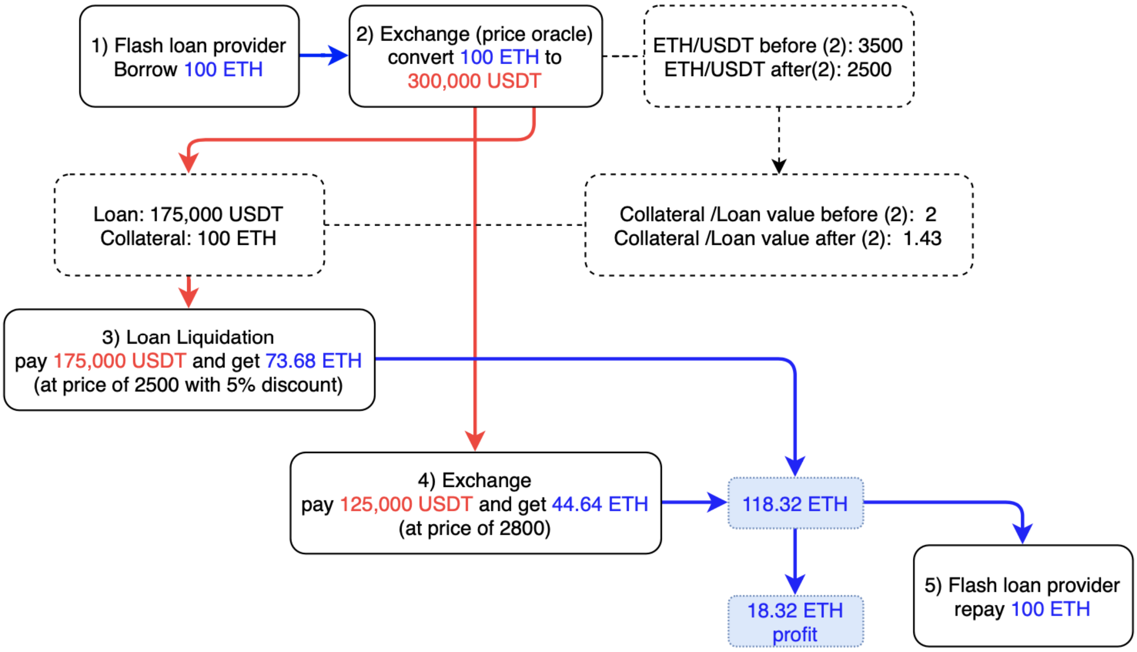

FIGURE 2.2: Price manipulation attack on a lending market

One might be curious who really lost money in this setup and who are the real victims. Well, the lending market is operating as it had been defined to protect lenders from losing money. Therefore, lenders and the lending market itself are not losing. On the other hand, the borrower's position had been liquidated, and his collateral had been sold at a discounted price. Obviously, the borrower in this setup is the victim, and the attacker had taken funds from his pocket.

CHAPTER 3

Some Defenses and their Shortcomings

3.1 Defenses

This chapter discusses ideas to make it more troublesome for an attacker to exploit a protocol. Ideas are around preventing flash loan based attacks; therefore, the attacker has to possess the funds to perform the attack (which is less likely).

3.1.1 Delay-based defenses

One may argue the problem arises because the hacker can easily change the oracle's price using a huge chunk of funds, fool the victim protocol and exploit it. Therefore, if a DeFi protocol uses lagged prices in its calculations instead of the current prices (aside from whether it is technically possible or not), price manipulation would be much more complex due to the fact that some agents call arbitragers will revert the prices to normal by just selling the mispriced asset in one market and buying it in another. Even if someone could keep the prices up or down for a block, it can not be done using a flash loan because of the fact that funds must be returned to the flash loan pool at the end of the transaction sequence or otherwise, the whole set of transactions would be reverted.

On the other hand, this defense might make some other frauds possible. In addition, it makes the protocol a bit lazy, although that would not be a considerable problem when block time is less than a minute.

Another option to produce some laziness to the protocol is to practice some commit-and-reveal mechanism. This idea would remove the ability to perform interactions with the application within a single transaction and, therefore, make a flash loan-based attack infeasible. On the users' side, this would mean that, for instance, during depositing, their tokens will be transferred into the DeFi in one transaction; subsequently, the users would claim their share in another transaction, ideally inside a different block. This method would constitute a UX change and potentially incur a higher, yet still acceptable, gas cost for the users.

3.1.2 Block flash loan funds

The number of flash loan providers on the Ethereum blockchain with enough funds to perform an attack is limited to four at the time of writing this report: Aave [1], dYdX, UniswapV2 [2], and UniswapV3. One simple but effective solution can be to directly prevent transactions involving funds from those addresses. Although this solution might seem totally complete, new flash loan providers might provide enough funds for a successful attack after all.

3.1.3 Off-chain price oracles

The problem that a blockchain is like a sandbox with no connection to the outer real world has been one of the most significant problems. Price feeds from centralized exchanges (CEX) are more reliable but not available in a decentralized way on a blockchain. Projects like ChainLink focused on providing off-chain data on the chain and make price manipulation more difficult[11]. Of course, this action would contradict the main idea of the cryptocurrency, a trustless system without any centralized authority. By relying on price feeds from a CEX, a DeFi protocol would make itself vulnerable to price manipulations from the centralized provider.

On the other hand, this solution would make price manipulation impossible using funds from flash loans. To do what it takes to change prices in a CEX, the hacker must deposit the assets. Deposit and withdrawal of the asset need to be in separated blocks; therefore, the off-chain part of the attack can not be done using funds from flash loans.

3.2 Defences Drawbacks

The proposed defenses are not complete, and one can find breaches to make the attack feasible again. This section is focused on how to use those holes.

3.2.1 Front running and network congestion

Any delay-based defenses can be ineffective in a network congestion situation. After submitting the malicious transaction, the hacker can broadcast multiple high fee transactions to bribe the miners to ignore other users' pending transactions, including arbitragers transactions that try to make the price manipulation useless. This kind of front running is applicable in a smart contract game called Fomo3D.[7]

Although the attacker can congest the network to make the delay ineffectual, it still blocks flash loan usage because the loan can not be paid back in the first block. Consequently, despite the defense is not totally complete, it makes it more complicated to practice the attack.

3.2.2 Crowdfunding smart contracts

Smart contracts can be audited by every node, and make sure that they will work as presented. A hacker with insufficient funds to practice exploitation on a DeFi might replace acquiring a flash loan part with a crowdfunding phase. This kind of crowdfunding is designed to allow multiple parties to collaborate in a trustless way on such an attack while keeping control of their funds and being assured that they will be compensated for their participation in it. If the required funds are not gathered by a horizon specified in the smart contract, investors on the attack are welcome to withdraw their assets.

Using a crowdfunding Smart contract eliminates the constraint of executing the whole attack in one block because the loan is not required to be paid back in a single block. This fact would make some aspects of delay-based attacks inefficacious and impotent. Although the crowdfunding idea reduces limits, it can not be used to manipulate prices in a CEX because one has to deposit their assets in a CEX to make a trade. Consequently, centralized price oracles defense is still succeeding.

3.2.3 Price anomalies on CEXs

On the Nov 26th of 2020, DAI/USDT price rose to 1.30 on Coinbase pro exchange.[6] This price anomaly led to about $90 million worth of asset liquidation on decentralized lending markets. Although it is much complicated to manipulate prices on a CEX, it has happened in the past and can happen in the future. The hacker must possess funds to do the manipulation, and despite it needs lots of assets, many so-called whales own that much.

On the other hand, the very same administrators of the CEX are able to trick the DeFi and exploit it. The main purpose of using a DeFi platform instead of a classical centralized party is to manage finances in a trustless system. By putting one authority to set the prices, the soul of the idea will be dead.

CHAPTER 4

Conclusion

This report presents an exploration of the impact of the flash loan mechanism on the Ethereum network and the idea behind price oracle manipulation attacks. While proposed as a clever mechanism within DeFi, flash loans are starting to be used as leverage to effectively exploit DeFi protocols. This report discusses existing defenses to some oracle price manipulation flash loan-based attacks and their shortcomings.

4.1 Future outlook

This paper only suggested approaches to protect funds against flash loan-based attacks. On the other hand, if the attacker owns the funds or obtains them in a way like crowdfunding, as mentioned earlier, he might still be able to perform the attack and exploit the DeFi. Future studies can focus on how to improve defense to be applied to scenarios where the attacker controls the funds as he wants.

Acknowledgements

I would like to express my special thanks of gratitude to my supervisor Professor Tang for being patient and helping me throughout the winter vacation program. I am moreover grateful to the University of Sydney for generously supporting the project through a scholarship.

Bibliography

[1] 'Aave Protocol'. In: (2020). Accessed: 2020-03. URL: https://github.com/aave/aave-protocol.

[2] Hayden Adams, Noah Zinsmeister and Dan Robinson. 'Uniswap v2 Core'. In: (2020). Accessed: 2020-03. URL: https://uniswap.org/whitepaper.pdf.

[3] Guillermo Angeris and Tarun Chitra. 'Improved Price Oracles'. In: *Proceedings of the 2nd ACM Conference on Advances in Financial Technologies* (Oct. 2020). DOI: 10.1145/3419614.3423251. URL: http://dx.doi.org/10.1145/3419614.3423251.

[4] Vitalik Buterin. *Ethereum: A next-generation smart contract and decentralized application platform*. Accessed: 2016-08-22. 2014. URL: https://github.com/ethereum/wiki/wiki/White-Paper.

[5] Yixin Cao, Chuanwei Zou and Xianfeng Cheng. *Flashot: A Snapshot of Flash Loan Attack on DeFi Ecosystem*. 2021. arXiv: 2102.00626 [q-fin.CP].

[6] Scott Chipolina. *Oracle Exploit Sees $89 Million Liquidated on Compound*. Nov. 2020. URL: https://decrypt.co/49657/oracle-exploit-sees-100-million-liquidated-on-compound.

[7] Shayan Eskandari, Seyedehmahsa Moosavi and Jeremy Clark. *SoK: Transparent Dishonesty: front-running attacks on Blockchain*. 2019. arXiv: 1902.05164 [cs.CR].

[8] Harvest Finance. *Harvest Flashloan Economic Attack Post-Mortem*. 2020. URL: https://medium.com/harvest-finance/harvest-flashloan-economic-attack-post-mortem-3cf900d65217 (visited on 26/10/2020).

[9] Lewis Gudgeon et al. *The Decentralized Financial Crisis*. 2020. arXiv: 2002.08099 [cs.CR].

[10] *harvest-finance*. 2020. URL: https://harvest-finance.gitbook.io/harvest-finance/.

[11] Mudabbir Kaleem and Weidong Shi. *Demystifying Pythia: A Survey of ChainLink Oracles Usage on Ethereum*. 2021. arXiv: 2101.06781 [cs.DC].

[12] Satoshi Nakamoto. *Bitcoin: A peer-to-peer electronic cash system*. 2009. URL: http://www.bitcoin.org/bitcoin.pdf.

[13] Kaihua Qin et al. *Attacking the DeFi Ecosystem with Flash Loans for Fun and Profit*. 2021. arXiv: 2003.03810 [cs.CR].

[14] Xinyuan Sun et al. 'How to Exploit a DeFi Project'. In: Sept. 2021, pp. 162–167. ISBN: 978-3-662-63957-3. DOI: 10.1007/978-3-662-63958-0_14.

[15] Dabao Wang et al. 'Towards A First Step to Understand Flash Loan and Its Applications in DeFi Ecosystem'. In: *Proceedings of the Ninth International Workshop on Security in Blockchain and Cloud Computing* (May 2021). DOI: 10.1145/3457977.3460301. URL: http://dx.doi.org/10.1145/3457977.3460301.

[16] Sam M. Werner et al. 'SoK: Decentralized Finance (DeFi)'. In: *CoRR* abs/2101.08778 (2021). arXiv: 2101.08778. URL: https://arxiv.org/abs/2101.08778.

[17] Jiahua Xu and Nikhil Vadgama. *From banks to DeFi: the evolution of the lending market*. 2021. arXiv: 2104.00970 [cs.CY].