Blockchain and decentralized finance (DeFi) are relatively new technologies.  This means that both have a certain lack of security maturity.  In recent years, hacks against DeFi projects have become commonplace, often yielding the attacker massive amounts of cryptocurrency.

Five of the twelve most expensive hacks to date have been flash loan attacks.  These attacks take advantage of the leverage provided by flash loans to allow an attacker to exploit vulnerabilities within DeFi projects’ smart contracts.

Often, these exploits allow the attacker to completely drain a project’s liquidity pools, racking up massive losses for the protocols’ users.  In many cases, these attacks are made possible by the same vulnerabilities within the projects’ smart contract code, making the attacks entirely preventable.

**INTRODUCTION TO FLASH LOANS**

If you take out a loan at a conventional bank, you need to provide collateral.  For example, mortgages commonly use the mortgaged house as collateral.  If the borrower defaults on the loan, then the bank can repossess their collateral.  Banks need collateral to protect themselves against losing money if a borrower defaults.  **Flash loans are designed to eliminate the need for collateral by making it impossible for a borrower to default on a loan**.

A transaction on the blockchain can actually include multiple different transactions, including value transfers and execution of smart contract code.  A flash loan is a transaction in which a user borrows some tokens, performs some actions using them, and repays the initial loan at the end of the transaction.

Flash loans eliminate the need for collateral because blockchain transactions are “all or nothing.”  If a transaction fails for some reason, the blockchain’s state is rolled back to the point before the transaction began and none of the actions included in it are performed.

It is impossible for a flash loan to fail in a way that allows the initial borrow to be performed without the final repayment executing as well.  This eliminates the risk to lenders and makes loans without collateral possible in DeFi.

Without the need for collateral, borrowers can get loans for much more than they could otherwise.  With zero risk of default, a lender can safely loan tens or hundreds of thousands of dollars in cryptocurrency to an unknown user.  The leverage that this provides makes flash loan attacks possible.

**HOW DEFI HACKERS CAN EXPLOIT FLASH LOANS**

In a flash loan, the initial loan must be repaid at the end of the transaction.  This limits what can be done with a flash loan because a user needs to be able to guarantee this payback.  Otherwise, the transaction will fail.

The most common use for flash loans is for taking advantage of arbitrage opportunities.  If a user can buy tokens at one value and sell them at another, there is the potential that they could end up with enough to pay back their initial loan and make a profit as well.

Arbitrage opportunities can happen naturally as different projects update their valuation of different tokens based on supply and demand.  In a flash loan attack, the attacker creates their own arbitrage opportunities by exploiting a vulnerable smart contract.

A flash loan attacker can do this by artificially modifying the relative value of a trading pair of tokens by flooding a contract with one or the other (using their loaned tokens).  The resulting difference in prices between the exploitable contract and the “real” value of a trading pair is called slippage.

By creating slippage, an attacker can acquire a token very cheaply or sell one at a high price to the exploited contract.  This enables them to drain value from the contract by forcing it to hand over the tokens deposited within it.  The attacker can then use other exchanges to convert their stolen tokens into the cryptocurrency of their choosing.

Additionally, this conversion process can be used to launder the attacker’s gains, reducing the probability that they will be locked into their account by various exchanges.

**THE BIGGEST DEFI FLASH LOAN ATTACKS**

Flash loan attacks are a common threat and enable hackers to steal massive amounts of cryptocurrency.  Some of the largest and most expensive flash loan attacks to date include:

* [PancakeBunny](https://halborn.com/explained-the-pancakebunny-protocol-hack-may-2021/): In May 2021, a bug in the price calculations for the BUNNY token was exploited to allow the attacker to steal $45 million from the protocol.
* [Alpha Finance](https://halborn.com/explained-the-alpha-homora-defi-hack-feb-2021/): In February 2021, the Alpha Finance project was hacked for about $37.5 million in tokens using a malicious contract that the Alpha Homora code was tricked into believing was an internal contract.
* [Spartan Protocol](https://halborn.com/explained-the-spartan-protocol-hack-may-2021/): Another May 2021 hack against the Spartan Protocol drained $30.5 million in tokens from the project by exploiting an incorrect calculation of liquidity shares.
* Harvest Finance: The Harvest Finance hack occurred in October 2020 and allowed the attacker to steal $33.8 million in tokens from the project’s FARM\_USDC and FARM\_USDT pools.
* [XToken](https://halborn.com/explained-the-xtoken-hack-august-2021/): A third hack from May 2021 makes the list.  The exploit against XToken drained over $24 million in tokens from several of the project’s liquidity pools.

At the time of publication, these five hacks are all within the top twelve most expensive hacks to date on [Rekt’s Leaderboard](https://www.rekt.news/leaderboard/" \t "_blank).  Flash loan attacks are common because they are easy for a hacker to perform and low-risk because the probability of exposure is so low (and in some cases the attacker is hired as a security advisor to the hacked protocol).  On the other hand, these hacks are expensive for an exploited protocol’s users and entirely preventable.

**PROTECTING AGAINST FLASH LOAN ATTACKS**

Flash loan attacks are made possible by contracts that perform their calculations of the value of a particular token or trading pair completely internally.  While using the contract’s supply of various tokens to determine price is the “purest” way of valuing assets, it also leaves these contracts vulnerable to manipulation and exploitation.

**The best way to protect against flash loan attacks is to use an external price oracle to protect against slippage.**  Smart contracts should update their prices based on their supply and demand for various tokens but should limit this price range based on external values.  Doing so makes it more difficult for an attacker to generate enough slippage to make an exploit profitable.

Flash loan attacks make up a significant percentage of all DeFi hacks.  This is not just an indication that the industry is failing to learn from its mistakes.  The vulnerabilities that make flash loan attacks possible are not always obvious and may require an in-depth security audit to discover.

The cost of a flash loan attack can be significant to a DeFi protocol and its users.  It has become commonplace for DeFi hackers to drain tens or hundreds of millions of dollars from DeFi protocols.

Before launching any smart contract, it is vital to undergo a security audit that can help to identify and remediate these and other vulnerabilities before they can be exploited by an attacker.  Halborn offers comprehensive audits of DeFi projects, including an in-depth review of smart contract code for vulnerabilities, like those that make flash loan attacks possible.

For more information on how to protect your project against these and other attacks, reach out to our security experts at [halborn@protonmail.com](mailto:halborn@protonmail.com).