[PDF Database Document] - BTCC Cryptocurrency Exchange

Original:
https://www.btcc.com/en-US/academy/crypto-basics/top-3-risks-of-defi-lending

Top 3 Risks of DeFi Lending

Whenever navigating any unregulated space, it's critical to understand the risks. Read this article to find out the top 3 risks of DeFi lending.

As with most things in the financial world, when something promises a very high rate of return, it usually runs into problems, and DeFi lending is no exception.

To put it simply, DeFi, shorthand for decentralized finance, is an ecosystem of blockchain-based applications that offer a range of financial services similar to those provided by traditional banks, insurance brokers, and other financial intermediaries. The main difference being, these decentralized applications, known as dapps, run autonomously without any third party acting in the middle. That's because each dapp is powered by a smart contract – a special computer program that automatically performs a function when certain predefined conditions are met.

DeFi lending is just one type of traditional financial service that is now accessible through these peer-to-peer operated dapps. Similar to depositing funds into a savings account to receive interest payments, crypto investors can now lock up their funds or use them to provide liquidity across a range of decentralized platforms and receive regular interest payments.

Many of the interest rates offered on these dapps are significantly greater than anything currently available in the traditional financial space, making DeFi lending a highly attractive passive income stream for crypto holders. But before lending any assets, there are a number of associated risks everyone should be made aware of.

Impermanent Loss Involved in Liquidity Pool

When you commit your assets to a liquidity pool, you risk something known as "impermanent loss."

Impermanent loss is when the price of assets locked up in a liquidity pool changes after being deposited and creates an unrealized loss (in dollar terms) versus if the liquidity provider had simply held the assets in a crypto wallet.

The change occurs for two reasons and has to do with the Automated Market Maker system DeFi liquidity pools use.

- DeFi pools maintain a ratio of assets in the pool. For example, an ETH/LINKpool might fix the ratio of ether and link tokens in the pool at 1:50 (respectively). Meaning anyone wishing to provide liquidity would have to deposit both ether and link into the pool at that ratio.
- DeFi pools rely on arbitrage tradersto align pool asset prices with the current market value, i.e., if the market price of link is $15 but the value of link in an ETH/LINK pool is $14.50, arbitrage traders will spot the discrepancy and be financially incentivized to add ETH to the pool and remove the discounted LINK.

When arbitrage traders flood the pool with one token in order to remove the discounted token – in this example, adding ether to take out link – the ratio of coins changes. In order to regain balance, the liquidity pool automatically increases the price of the token in higher supply (link) and reduces the price of the token in lower supply (ether) to encourage arbitrage traders to rebalance the pool.

Once the pool rebalances, the rise in the value of the liquidity pool is often less than the value of the assets if held by the lending protocol. That’s an impermanent loss.

Here’s a summary of the graph’s data and the relationship between price change and percentage loss:

1.25x price change = 0.6% loss

1.50x price change = 2.0% loss

1.75x price change = 3.8% loss

2x price change = 5.7% loss

3x price change = 13.4% loss

4x price change = 20.0% loss

5x price change = 25.5% loss

In defense of these protocols, liquidity providers (LPs) are rewarded with a proportionate amount of trading fees for adding assets to the pool, which can often offset impermanent losses. Uniswap, for example, charges a flat trading fee of 0.3% which is distributed to LPs.

Top tip: The best way to mitigate impermanent losses is to provide liquidity to pools containing less volatile assets such as stablecoins.

Impermanent loss shouldn't be something that scares you away from DeFi lending, but rather a calculated risk to understand before lending your assets.

Attacks from Flash Loan

Flash loans are a type of uncollateralized lending unique to the DeFi space. In the traditional, centralized model of banking, there are two types of loans:

- **Unsecured loans**: These require no collateral because they are typically smaller amounts of money, think a few thousand dollars.
- **Secured loans:**These are larger and require collateral like a property, car, investment, etc. Throughout the entire loan process, banks have tools to assess the credibility of clients, like credit scores, reports, and so on.

Flash loans are a type of unsecured loan that uses smart contracts to mitigate all the risks associated with traditional banking. The concept is simple: A borrower can receive hundreds of thousands of dollars in crypto assets without putting up any collateral but the catch is they have to pay the full amount back within the same transaction it was sent (usually a few seconds).

If the loan isn't paid back, the lender can simply roll back the transaction, like it never happened. Because there's zero risk involved in issuing these types of loans, there is no limit to the amount a person can borrow. And because the entire process is decentralized, there are no credit scores or reports preventing a person from qualifying for a flash loan.

Flash loan attacks are when bad actors borrow huge sums of money using these special types of loans and use them to manipulate the market or exploit vulnerable DeFi protocols for their own personal gain.

A flash loan attack against the yield-farming aggregator PancakeBunny made headlines when the attackers caused the price of PancakeBunny's token, BUNNY, to drop 95%. They did this by borrowing large amounts of BNB through the PancakeSwap lending protocol, manipulating the price of BUNNY in off-market lending pools, and then dumping that BUNNY on the open market, causing its price to crash.

As is the case with almost all flash loan attacks, the thieves escaped without repercussion. It's estimated the attackers netted $3 million in total.

Once a liquidity pool is drained of a particular token, liquidity providers can become exposed to impermanent loss. Not to mention, lesser-known tokens hit by these attacks – such as BUNNY – cause investors to lose all confidence in the projects and they rarely recover in price.

Rug Pulls of DeFi

Without traditional forms of regulation in the DeFi lending space, users have to develop a certain degree of trust with the platforms they're willing to lend their assets to or buy tokens from. Unfortunately, that trust is often breached in the form of rug pulls.

Rug pulls are a new type of exit scam where DeFi developers create a new token, pair it to a leading cryptocurrency such as tether or ether and set up a liquidity pool.

They then market the newly created token and encourage people to deposit into the pool, often promising extremely high yields. Once the pool has a substantial amount of the leading cryptocurrency in it, the DeFi developers then use back doors intentionally coded into the token's smart contract to mint millions of new coins that they use to sell for the popular cryptocurrency. This completely drains the popular cryptocurrency from the pool and leaves millions of worthless coins in it. The founders then disappear without a trace.

A famed "billion-dollar rug pull" came in 2020, when SushiSwap developer Chef Nomi unexpectedly liquidated his SUSHI tokens after raising over a billion dollars in collateral. The price of the Uniswap competitor's token fell to near zero in what is remembered as one of "the most dramatic moments in DeFi."

DeFi fraud is a billion-dollar industry and, despite efforts to mitigate risks by developers, remains a prevalent aspect of the growing space. It was reported that the first half of 2021 brought triple the volume of DeFi hacks and fraud compared to 2020 altogether.

How to Avoid These DeFi Lending Risks

Despite the rampant increase in this type of malicious activity, there are methods to vet a company for potential exit scams before investing. These include:

- Verifying the team’s credibility on other projects.
- Diligently reading through a project’s white paper.
- Checking to see if the project’s code has been audited by a third party.
- Being acute to potential red flags – like unrealistic projected returns and overspending on promotions and marketing.

Ultimately, the same permissionless design that makes DeFi protocols vulnerable to theft is the source of their potential to disrupt the financial industry. The combination of limited regulatory oversight and the open source nature of the blockchain means that lending protocols that handle large sums of money will always be vulnerable. As with almost all sectors of the blockchain industry, the goal is to mitigate these risks over time.