Hackers Opinion: DeFi Should Emulate the Concept of Traditional Finance

Original: https://www.btcc.com/en-US/academy/research-analysis/hackers-opinion-defi-should-emulate-the-concept-of-traditional-finance

Hackers in the world of DeFi always appear in the news. Kate kurbanova of apostro said that the DeFi protocol should start using the risk management rule sets and tools already used in traditional finance.

A loophole in the smart contract can cost the DeFi project millions of user funds. Although technical loopholes and errors are the first attack carrier hackers are looking for, people cannot forget other means used to steal funds from the DeFi protocol.

Formal verification, stress testing, auditing and Simulation – there are a large number of practices and tools to choose from in the technical audit and thorough inspection of code errors and hidden vulnerabilities.

However, even all the above practices can not guarantee the security of the protocol, because some vulnerabilities come from the defects of product business logic and dependence on external markets and DeFi components. These are so-called economic loopholes – they require additional economic audit and are generally more difficult to capture, because this space is evolving and any code upgrade may lead to new utilization possibilities.

Therefore, the field of DeFi security needs to be upgraded and better risk management practices need to be adopted to protect users and protocols from economic threats.

Hacker Attacks Continue to Loom

Over the years, many protocols have been used, and the most common attack vectors have been recorded and patched. Nevertheless, there are ways to use agreements by indirectly affecting the logic of the contract or the business logic of the agreement. This may be a possible backdoor caused by market or Oracle manipulation, affecting connection protocols or continuous monitoring of code upgrades.

Such vulnerabilities may use multiple protocols throughout the execution process. In particular, one possibility is to use lightning loan attacks to manipulate the price Oracle of the agreement. In order to better understand it, we can study a specific example.

Loopholes in Flow Finance

This occurred in November 2021, resulting in a loss of $130 million. The attacker manipulates the price of yUSD by exaggerating liquidity and using the price Oracle, which leads the system to believe that 1 yUSD is equal to $2. The cost of yUSD initially deposited by the attacker is $3 billion. The hacker then converted his yUSD deposit into $3 billion and used $1 billion in profits to consume all cash finance's liquidity (about $130 million).

Beanstalk

Another recent hacker exploited a vulnerability in Beanstalk's governance system. Hackers used a back door in the governance of the agreement and obtained two-thirds of all governance powers through lightning loans. This enables them to implement the governance proposals they create with a one-day delay (rather than the seven-day delay typically required for reviews).

These seemingly safe proposals turned out to be a malicious contract. This was activated at the time of the flash loan, which basically exhausted $182 million in the agreement (when used).

Both attacks exploit the business logic of the agreement by abusing the economy behind the agreement. These types of attacks show how important it is to have risk management tools and continuous monitoring because they can easily capture and prevent such opportunities.

Using Risk Management Tools to Enhance Safety

In order to provide an additional security layer to prevent such attacks, the DeFi protocol should begin to use risk management rule sets and tools, which has been proved by the practice of

traditional financial circles for many years.

For example, one method here is to implement the time delay of the transaction in the protocol. Such a function can delay suspicious transactions in the protocol, remind developers of malicious activities, and give them time to mitigate the negative impact (if any). This can be further improved by combining delay with monitoring tools to automatically delay or suspend transactions that pose a threat to the protocol.

Another good practice is a liquidity ceiling – limiting the amount of money that can be transferred in a transaction. Although it will not affect ordinary users, the mobility ceiling can delay or prevent attacks similar to the cream finance vulnerability, because it makes it more difficult and expensive for hackers to run attacks.

The field of DeFi security can benefit a lot from the network security expertise of traditional finance, because it will bring more expertise and experts to achieve higher security and stronger infrastructure of Web3 protocol.

Hackers in DeFi

Although the rapid growth in the field of DeFi is attractive to ordinary users and investors, the lack of security practices and solutions is still the main disadvantage of wider adoption and institutional investors.

When it comes to their financial security, ordinary viewers need more assurance – knowledge and practice from traditional finance can push the DeFi scene to a new level of development. Using risk management tools, operational safety practices, safety caps and continuous monitoring – the field of DeFi can greatly benefit from the correct application.