**Strengthening the Security of DeFi Solution**

Decentralized finance has been effective in gaining the confidence of investors. However, there are many questions about the dependability and safety of decentralized financial technology as a result of DeFi security vulnerabilities related to the increasing frequency of recent protocol assaults.

**ADVANCED DEFI HACKS**

According to DeFi Pulse, the TVL locked in DeFi is growing quickly and has now surpassed $12B. Hackers looking to make a killing are quite interested in this rapidly expanding business.

**CLASSIFICATION OF DEFI ATTACKS**

Unfortunately, we can even categorize "a big win" attacks given their impressive prevalence. Even if there hasn't been a similar DeFi protocol breach, there are some similarities in the protocol's weaknesses.

**Vulnerability of code**

The first class of DeFi protocol hacks is carried out purely as a result of code errors. These result from hastily conducted security audits or even from undetected smart contract flaws. Unfortunately, many owners of blockchain projects opt to operate their projects with minimal unit test coverage and forego performing smart contract security audits. This significantly increases the risk of assault and financial loss.

**Advanced contract logic**

The following form of DeFi project hacking targets the entire smart contract logic rather than the usual code flaws. The belief that a proper contract trial on a test net may lower the likelihood of such an assault is frequently held but not necessarily by those who do not witness it.

**Fewer smart contract weaknesses minimize Defi hacking**

Generally speaking, auditors and protocol developers may miss a hacking chance because they lack expertise and business process understanding. When working in a field like DeFi, understanding traditional financial tools and how they are used is essential.

**How can your DEFI project be protected against hacking?**

Well, there are enough flaws in the current DeFi initiatives to be found.

**1. COVERAGE OF ALL UNIT TESTS**

Any top-notch project testing must include unit tests. These aid in identifying functionality issues in various contract components and eradicating them from the outset. What matters is that the contracts call for comprehensive unit test coverage, not only testing "the most crucial sections of code."

**2. SMART CONTRACT SECURITY AUDIT**

However, even if you tested every method, class, and module, it does not ensure that your contract is error-free. Since the whole unit test coverage cannot cover all potential user pathways and permutations, a security audit must be thought of as the following step. Before a project is implemented, auditing assists in identifying unequal and unanticipated smart contract vulnerabilities, helping to stop DeFi hacking.

**3. SUPPLEMENTARY AUDIT**

The dForce protocol hack is an excellent illustration of why one audit is insufficient before project release. Although the ERC-777 token standard is thought to be less prone to attack, this does not guarantee a seamless connection with Lendf. me. The same applies to the launch of imBTC (used in this attack as well). They could have prevented such a terrible situation if they had audited all potential functionalities.

**4. UNIQUENESS OF CODE**

Using the dForce example as a guide, it is clear that copying and pasting code from other protocols is not a good idea. Simply said, if you don't fork the entire blockchain project, you'll try to "fit in" certain pieces of code, which frequently won't work with what you currently have. Future exploits will mostly be committed for this purpose.

**5. DEFENSE OF ACCESS UNDER CONTRACTS**

We strongly advise adopting the multisig method to prevent unauthorized access to your private key or to safeguard your DeFi protocol if your key is lost. Developers may do this in one of two ways: first, by creating a distinct multisig contract; second, by incorporating multisig logic into your protocol.

**6. A TEAM OF EXPERIENCED DEFI DEVELOPERS**

As you can see, cybersecurity concerns need to be considered even before the project is developed. Therefore, it is imperative to hire a group of skilled blockchain engineers who are knowledgeable about the risks and requirements of the DeFi project.

**7. TURN TO THE COMMUNITY**

Developers advise consulting your protocol community as a last resort. It's important to take all those actions to reduce any security threats already there, but you may improve the outcome by enlisting the aid of a committed audience. By offering a bug reward, users will be encouraged to report any problems they find. As a result, you gain from enhancing the protocol's user experience and successfully defending against DeFi attacks.

**CONCLUSION**

DeFi is unquestionably one of the most potent crypto fields in use today. This is a desirable location to invest and significantly raise your wealth. However, nothing ventured, nothing gained, therefore every gain encounters obstacles along the route.

As you can see, there is a list of these drawbacks and DeFi security flaws. We think that each project owner should be aware of them and take timely action to eliminate them.