**Qubit Finance Hack Post-Mortem: The Trail the Hacker Left Behind**



Another day in crypto and another hack. This time X-Bridge was exploited and the hacker stole $80 million worth of tokens. This is the second biggest hack so far in 2022. Last year saw a total of [over $10 Billion in lost funds](https://assets.ctfassets.net/t3wqy70tc3bv/1Uu42jJx49FHXleMESH2Ii/600bd8f4fafaaac4890bc4fa258cc243/Immunefi_Top_Hacks_In_2021.pdf) due to hacks. This is hindering crypto adoption and it must be addressed. A deep dive into how the hack happened and how exploits should be prevented in the future.

Qubit Finance is the operator of X-Bridge. This is a cross-chain bridge between Ethereum and Binance Smart Chain that enables easy token swaps from one to the other. For example, you can use a wrapped ETH token and transform it into a qXETH token, which allows you to use Ethereum in the Binance Smart Chain ecosystem.

**How did the hack happen?**

The hacker found a way to trick the Smart Contract and make it believe it received wrapped Ethereum while it didn’t. Afterward, the hacker used those non-existent funds and turned them into real funds, and transferred those real funds to their wallet on the Binance Smart Chain.

Let’s start with the basics. A smart contract is built up with functions. These get initiated when you as a user interact with the protocol. Hackers analyze the code of these smart contracts and try to find a loophole.

In this case, the hacker tricked the function that allows users to swap tokens within the protocol from one blockchain to another. The condition for this function to be triggered is logically that you need to deposit first and after you can swap the deposited token into another token and withdraw it.

A function needs certain inputs in order to be able to be executed. Examples of inputs are the token you deposit and the token you want to swap towards. Another input for this function is the wallet address that you use to deposit the funds. The hacker included instead of their own address, a whitelisted address. Whitelisted addresses are recognized wallets by the protocol to do transactions with. Using this address allowed the hacker to execute the function to mint qXETH and withdraw it without depositing the wETH.

Normally when the function would recognize that there were no funds deposited, it would fail, however, because of this whitelisted address, the transaction didn’t fail. The hacker did several rounds of this and in the end, gathered a large amount of qXETH on the Binance Smart Chain. Finally, the hacker sold that qXETH for BNB.

This hack was allowed to happen because of a mistake left by the developers of Qubit Finance. There was a loophole in the code that could have been prevented.

Qubit Finance responded the next day and released a short blog post where they explained how the hack did occur. They [shared the steps the hacker took](https://medium.com/@QubitFin/protocol-exploit-report-305c34540fa3) and the functions they used to obtain the $80 million. They also committed to releasing the maximum bounty of $250 000, if the hacker were to return the funds.

The volumes of X-Bridge have fallen significantly since. A few days prior to the hack, daily volume peaked at $60 million. Since the hack, volumes have typically been far below $1 million per day. Hacks really [damage protocols](https://dappradar.com/binance-smart-chain/defi/qubit-finance) and it is extremely hard to recover for them as a crypto project.

**How to avoid such hacks?**

Prevention is always the first thing to focus on as a protocol or user. This can be done by hiring top security and auditing firms within crypto to review the code and take out the loopholes. However, it is always possible that something was missed.

Compare it with a car — it is designed to be very safe and the environment around it is designed like that as well. There are traffic signs, every driver needs a driver's license and there are regulations around the quality of cars. However you can never prevent all accidents, therefore we all wear a seatbelt, so when an accident happens, we have a higher likelihood of surviving the accident.

Lossless is such a seatbelt for crypto protocols. Once a hack occurs, the Lossless smart contracts which are integrated into protocols, allow freezing the suspicious transaction and kickstart a process to review it. The Lossless decision-making body, composed of external experts, Lossless team members, and representatives of the affected token decides whether the transaction can go through or not. An investigation is made in 24–48 hours. When a transaction is indeed malicious, the Lossless protocol receives 7% of retrieved funds and 2% is given to the first one to uncover the hack.

It is critical that the crypto industry focuses on the safety of funds. Open blockchain systems have tremendous potential and in order to achieve that, the whole world needs to get onboard. A big roadblock is hacks and potential users being afraid of trusting a crypto protocol with their assets. The average person is not able to review code and make an informed decision on the quality of the smart contracts.

Lossless is already integrated into over 20 crypto projects. Cyber security is rapidly moving from a nice-to-have to a must-have. Reach out to us today to make your protocol safer and more valuable to your users.

**About Lossless**

Lossless is the world’s first DeFi hack mitigation tool for token creators. Apart from our known cyber security solutions and renowned professionals, the community also plays a role. With a tangible reward system, community members are also encouraged to explore new ways to detect hacks and fraudulent transactions.

Our [protocol](https://link.medium.com/Vo5LOHQWSkb) halts counterfeit transactions through various methods of fraud identification and automatically reverses any stolen tokens back to the original owner. Our solutions to the impending problems of cyber theft within the blockchain space are thorough and applicable within many protocols.