

Profitable INVESTING Tips

Stock Market Investing Tips, Techniques, and Resources



Anatomy of a Blockchain DeFi Hack

By: www.ProfitableInvestingTips.com

The culprit has the money and Indexed Finance is short millions of dollars in crypto currency. How did this happen and what does it portend for the future of the blockchain, decentralized finance, and your personal crypto assets? The anatomy of a blockchain DeFi hack shows us how one 18-year-old math whiz can slip into a blockchain system, raise havoc and leave with their ill-gotten gains. An argument for cryptocurrencies, decentralized finance, and the blockchain is that they do not rely on the standard financial institutions and regulators. An argument against them is that when money goes missing there is often nowhere to turn for help. The case will eventually end up in court where the culprit, if he shows up, will argue that he simply used the system's own algorithms to trick it into creating the conditions that allowed him to make money.

How the Blockchain Theft Played Out

Bloomberg covered this [crypto platform hack](#) a couple of months ago. The theft happened in the fall of 2021. It involved Indexed Finance which operates a crypto platform which creates tokens which, in turn, represent baskets of other tokens. You can think of an index fund within a blockchain. An employee of Indexed Finance spotted a suspicious trade in which one of the blockchain's users had purchased substantial amounts of various tokens at very reduced prices. This would be like going into an S&P 500 ETF and getting a 90% discount on purchased shares and no one noticing.

The employee passed the information to those in charge. Because the blockchain records and stores all information the programmers at Indexed Finance and their associates were able to see what happened in detail but it took about three weeks of digging to get there. The hacker had managed to trick the system into undervaluing tokens owned by users and selling them to the hacker at substantial discounts to their market prices. The sum total of assets made off with about \$16 million in crypto assets at the then-current market valuations. The code has been fixed and there have been no more hacks of that sort.

Who Pays for a Blockchain Hack?

After fixing the "hole in the code dike" the folks at Indexed Finance no longer had active losses but then had to deal with not-very-happy customers who had lost money. As a practical matter when these sorts of hacks occur the folks who lost money can often track down the culprits. What commonly happens is that a deal is struck. The hacker keeps a portion of their ill-gotten gains, and all is well. In this case the culprit disappeared after leaving some choice words for the folks who got hacked. He is still available to chat by email and two lawsuits have been filed against him. Unlike with a US bank account there is no Federal Deposit Insurance for crypto assets so those who lost in this case will need to wait for the court and to see if any assets remain.

The Frailty of Automated Market Makers in the World of Blockchain

Indexed Finance uses an automated market-maker program to maintain balance of assets within their system. Pool prices were automatically adjusted to provide incentive for customers to buy or sell as desired. The hacker in this case studied the system and even worked with them briefly with the promise to create useful apps for them. The system devised by Indexed Finance saved money by not using live people in the process of adjusting prices. This saved management fees up to 1% such as are charged by rival Index Coop. The system did not check prices in the outside world but rather consulted its benchmark token which as the largest token in the pool.

Hacker Takes an Interest in Indexed Finance and Its Automatic Market-Maker

According to *Bloomberg* the hacker, with whom they are in contact via email, decided to play with the system to see if he could make money by manipulating the program's algorithms. A math whiz, he spent hundreds of hours manipulating the math involved and then devising bots that could execute trades, make money and even make the system function more efficiently. Along the way he realized that there was a "mispricing opportunity" that he could exploit. It included getting around safeguards meant to limit the size of trades.

In October of 2021 the hacker saw his opportunity with two Indexed pools "ripe for reindexing." The process required hundreds of commands and boiled down to creating very sudden over-supplies of token that forced the system's programming to re-adjust prices which the hacker then took advantage of. He did not change any of Indexed Finance's code but rather manipulated how their system worked. The Bloomberg article explains this in detail.

In communication with Bloomberg the hacker expresses surprise that his plan worked out so well. When indexed filed a lawsuit in Ontario where the hacker comes from, they found there was already a sealed lawsuit by the largest holder of token who lost assets. The court has frozen the tokens so the hacker will be breaking the law if he moves them. Indexed Finance argues that two specific steps in the hacker's process were in violation of computer hacking and market manipulation laws as the only purposes of some of the trades in the process were to distort pricing for the hacker's profit. They also claim that the hacker intentionally overwhelmed the system's security protocols. In Canada any action subverting the intended purpose of a security system is legally a hack.

While the hacker has not responded to the lawsuits and contends that he does not even have a lawyer in Ontario he contends in his emails that he executed perfectly legal trades. He did not gain access to any part of the system where access was not allowed. He did not steal private keys. Rather, he says, he interacted with the system and beat it using its own rules. He contends that others who had tokens in the system also use the system's smart contracts to their own advantage but that he did it more efficiently and profitably. He goes on to note that those who lost were operating in a system that they did not understand.

A law professor interviewed by *Bloomberg* notes that folks on Wall Street routinely make a lot of money in a hurry when they exploit a gap in pricing. This success is commonly preceded by lots of strategic and tactical research, similar to what the Indexed Finance hacker did. One of the outcomes of court action might be that this is viewed as a highly speculative trading scenario that turned out to be spectacularly successful.

Regulation of DeFi

A substantial amount of [regulation](#) is about to descend on the crypto, DeFi, blockchain world. The heads of the SEC and Commodity Futures Trading Commission have promised regulatory action and have described the current marketplace as violating statutes in commodity trading. Some of the murkiness of situations like this may be cleared up. In the meantime those who have piled into the decentralized and unregulated world of crypto, DeFi, and the blockchain may simply have to lick their wounds and fight another day.

After the lawsuit was filed the hacker appeared with camera off and the judge ordered him to either show up in court or transfer the disputed assets to a third party. He did neither and the judge issued a warrant for his arrest. When investigating blockchain investment opportunities one may wish to consider the [security of the system](#) that underpins your blockchain DeFi investment.

For more insights and useful information about investments and investing, visit www.ProfitableInvestingTips.com.

Educational Resources

**Click the links below to get your
FREE training materials.**

Free Weekly Investing Webinars

Don't miss these free training events!

<http://www.profitableinvestingtips.com/free-webinar>

Forex Conspiracy Report

Read every word of this report!

<http://www.forexconspiracyreport.com>

Get 12 Free Japanese Candlestick Videos

Includes training for all 12 major candlestick signals.

<http://www.candlestickforums.com>

Disclaimer: Trading and investing involves significant financial risk and is not