虚拟货币具有去中心化的特点，理论上不存在被盗的可能，但无数事实告诉我们，只要有交易，黑客有无数种方式盗窃虚拟货币，并不一定要破解加密货币。

该公司使用一种被称为MonoX的去中心化金融协议，交易双方通过名为“Mono”代币进行交易，大体过程为：

1.检查兑换参数是否正常

2.计算应输入输出代币的数量以及代币兑换后的价格

3.执行兑换操作，并将新的代币写入账本

在不同代币兑换时，上述过程能正常运行，但在同种代币兑换时，则出现了两个问题，在执行第二个步骤时，没有考虑兑换过程中，交易池代币储量的变更。最后一步没有考虑同种代币进行兑换时，兑出代币的价格更新操作会覆盖兑入代币的更新操作。

这个例子在现实中根本无法成立，因为他们俩在那边倒来倒去，鸡蛋的价值还是5块钱，太贵根本没人买，或者人们就会寻求其他替代品，比如吃鸭蛋。到头来，张三的鸡蛋还是只能以5元一斤的价格往外卖。

问题是计算机程序不是人，它只会执行人类为它事先设定好的操作。按照设定，李四以每斤7块钱的价格向张三买鸡蛋后，计算机程序认为张三的鸡蛋都值7块钱，而且不会买一斤少一斤，原来多少还是多少。

100块钱一斤的鸡蛋，不会有人买，但计算机程序会照单全收，就产生了这么一出闹剧。

用Mono代币买Mono代币本来应该被禁止。假如有一家公司对外宣布，本年公司流水高达3万亿美元，结果一调查发现，这家公司根本就是空壳公司，之所以有这么高的流水，是通过拿1万美元去买1万美元，反复操作来的。

在会计行业，像这种操作不具有商业实质，是不能确认收入的。但MonoX协议却允许这种操作……

更让人无语的是，MonoX在今年已经接受了三项安全审计，均没有发现这一低级漏洞。

MonoX并不是唯一的受害者，十月份，黑客利用Indexed Finance公司其重新平衡

指数池方式进行攻击，损失约1600万美元。区块链分析公司Elliptic所谓的DeFi协议已经损失120亿美元。

因为底层技术不成熟，使黑客能够轻易窃取用户资金，而流动性池使犯罪分子能够清洗勒索软件和诈骗等犯罪所得。