作者： Kaili Wang

来源： mirror

区块链交易不可变现是福是祸。

BAYC钓鱼网络攻击。 网络黑客。 黑客入侵。 Ronin盗窃案。
仅2021年就有140亿美元的加密货币被盗。
这些——和更多的3354是确实的盗窃行为，但没有“取消按钮”。
(例如，信用卡支付逆转) )。不是每个人都有根据需要拯救他们的跳跃crypto。

但是，如果有可逆类型的令牌呢？

斯坦福大学的几个研究者(Dan Boneh，Qinchen
Wang和我)这几个月来努力回答的问题。 我们设计了接近ERC-20和ERC-721的选择式令牌标准，支持逆转交易(在有充分证据支持逆转交易的情况下)，写了关于它们的论文，也实现了一些原型。 这些令牌的标准分别称为ERC-20R和ERC-721R。

现在，你可能在考虑“可逆令牌” ？ 这不是违背了区块链的目的吗？
实际上没有。 它并不意味着取代ERC-20令牌或使以太网成为可逆——。
只会在交易后的短时间内对盗窃行为提出质疑，并有可能恢复。

注意，交易在不可逆之前只能冻结很短的时间(例如3天)。
ERC-20R资金大部分时间都不可逆转。

交易中可逆性

交易中、两个可逆令牌之间的交换是即时的；
如果一方要求冻结，无论是否超过可逆时间段，都有可能从另一方回收资金。
然而，可逆令牌可以被交换为不可逆令牌；
为了保护自己免受逆转，交易只有在可逆时间段后才可能最终完成交换。
也就是说，可逆不可逆的交换在资金无法逆转之前会有延迟。
因此，当两个主要令牌可逆时，其他令牌也会在很大的压力下可逆。

根据实施情况，能够立即清算超过可逆时间段的资产(例如，清算3天前接收的资产)。 在这种情况下，你的可逆令牌和不可逆令牌之间没有延迟。

工作原理

逆转交易的过程

假设攻击者从受害者那里窃取了资金。
如下图1所示，资金可能进一步转移到其他地址。

1、被害人可能要求冻结被盗资金。
受害者向管理合同提出冻结请求，同时提出相关证据和一些资金。
有争议的交易必须是最近发生的(有一定的可逆时间段)。

2、法官接受或拒绝冻结请求。 投票中央化法官小组决定是否冻结资产。
审议时间最多一两天。 如果他们拒绝了请求，程序将停止，受害者将失去资金。
如果他们接受了请求，治理合同将冻结ERC-20R/ERC-721R合同。

3、执行冻结。 NFT的情况那只会阻止NFT被转移。
对于ERC-20R，跟踪被盗资金，并禁止移动这些资金。
请注意，只要账户所有者的余额高于被冻结的金额，就可以与他人进行交易。

4、审判。 然后呢双方都可以向中心化的法官小组提交证据。 最终，法官做出了决定，指示治理合同调用受影响的ERC-20R或ERC-721R合同上的reverse或rejectReverse函数。 调用rejectReverse将解除对争议资产的冻结。
审判时间可能会变长，也可能会持续几个星期。

5、逆转(如果适用)。 reverse函数将被冻结的资产送回受害者。

资产被盗时，很少放在一个地方。 攻击者经常将其从一个账户转移到另一个账户。
在这种情况下，攻击者还可以监视内存池(mempool
)，看到冻结请求已收到，然后通过先占交易转移资产。 为了避免这种情况，解决方案是在一次交易中执行完全的链式冻结(及其计算)，防止攻击者“跑”过冻结。

但是，接触到这些资产的所有账户都不能直接失效。
那么，你怎么决定冻结哪个账户？ 幸运的是，对于NFT，冻结非常简单。
只需确认目前拥有NFT的人并冻结帐户即可。
但是，货币的分割性使ERC-20的冻结更加复杂。 这些资金可以分成几十个账户、Tornado之类的匿名混音器，或者兑换成其他数字货币。
如果它通过了很多账户，至少有些账户和黑客有关。
但是，一些账户很可能是无辜的，或者是提供合法服务以换取支付的商家。
我们不能总是准确分辨所有账户的罪孽。
因此，我们提供了跟踪和锁定被盗资金的默认冻结流程。 我们的算法保证

1、假设没有销毁，足够的资产将被冻结以弥补被盗金额。
【销毁的资产从返还的金额中扣除】

2、账户中的资金只有在与小偷有直接交易的情况下才会被冻结

3、对于交易图，该算法的运行时间复杂度是合理的

我们在论文中讨论了更多的算法细节。

去中心化的司法系统

这个谜题中更模糊的部分涉及“去中心化的法官组”。 这些法官是谁？
他们怎么投票？ 他们怎么得到报酬？

它们最终取决于治理，即创建ERC-20R/ERC-721R实例的人。
我们的论文讨论了如何阻止法官的不诚实、贿赂、报酬制度等。
法官强调不能增加交易，也不能任意修改一个人的余额值。