Axie Infinity 游戏页面。| 来源：NBC News

遭受黑客攻击的 Ronin Bridge，正是游戏公司为 Axie 生态所创建的跨链桥，方便玩家在不同的区块链之间发送和交换游戏代币，绕开以太坊上昂贵的交易费用。

有了 Ronin Bridge，原本无法实现的资金跨链传送变得操作「丝滑」。

多链世界里，跨链桥是重要的基础设施，就像现实世界中的互联网和道路交通一样。跨链桥可以连接不同的区块链系统，允许用户在不同的链之间传送和交换代币。

简单来说，跨链桥可以将资产从一个区块链转移到另一个区块链，打通不同区块链系统间的操作。

在跨链桥上，资金往来是一件很平常的事情。Axie
游戏公司很可能
把黑客的操作误以为是用户正常的存取款行为，再加上缺少完备的合约余额监控系统，没有第一时间发现攻击行为。

生意上的精明，踩中了技术安全的坑。

被盗的「钱」去哪了？

埃文斯是幸运的，他没有因为黑客攻击而有真正的金钱损失——他持有的游戏货币

和原来数量一样，只不过暂时没办法从游戏中提款。

但不是所有玩家都像他一样走运。黑客攻击 Ronin Bridge 之后，窃取了 17.36 万枚 ETH 和 2550 万枚 USDC，价值 6.25
亿美元。这些被盗走的「钱」，去了哪里呢？

区块链安全公司 CertiK（公众号
ID：certikchina）高级工程
师王沛宇告诉极客公园，这些钱被黑之后，全部去到了攻击者的一个钱包地址里。

攻击者每隔几天就会从钱包里拿出来一部分钱，转进
mixer（混币器）或一个可以被认为是用来「洗钱」的工具 Tornado Cash。

截至北京时间 5 月 4 日，被盗资金几乎全部被转走，原来的攻击钱包里只剩下 1.8 枚 ETH。

V 神认为跨链桥存在基本的安全限制。| 来源：Twitter 账号 @VitalikButerin 截图

跨链桥成为区块链安全的软肋，需要从两个概念谈起：链上交易和跨链交易。

CertiK 工程师杨源楠介绍，这是两种完全不同性质的交易。链上交易依赖区块链算法的共识机制——已经被理论和实践验证过安全性。如果将区块链看作一个系统，单独的链上交易只是在系统内进行数据更新，达成共识。

跨链交易则不然。一个「跨」字，打破了区块链间的壁垒，也意味着「桥」两端的不同
系统需要
在一定程度上保持
更新一致，而这两个系统可能存在很
大差异。
由于每条链的设计都只能保证链上交易，跨链交易需要依赖很多额外的机制，比如对链上信息的监听、处理和发送，复杂性和难度远大于链上交易。

例如，在同一家银行转账方便易操作，但如果想把钱转到其他银行，甚至境外银行，不仅流程复杂，还有手续费。

跨链桥在这中间的作用是，保证两个不同系统之间资金变化的正确性和一致性。

举例来说，要将以太坊上的 10 个 ETH 转移到币安链，跨链交易的流程大致包括：

- 以太坊端的桥合约收到 10 个 ETH 后，发布一个转账消息；
- 跨链网络监听到这个消息；
- 跨链网络调用在币安链端的桥合约，提供与 10 个 ETH 等值的币给用户。

整个过程涉及三个相互联系但相对独立的个体：以太坊上的桥合约，跨链网络和币安链上的桥合约。它们分处于不同的
平台上，相互之间只是通过消息传递机制来保证数据在链间的传输。

跨链项目本身是一个复杂的系统，这里的核心就是消息传递机制。一旦这个机制存在漏洞，就可能成为黑客伪造跨链消息从而发起攻击的关键。

跨链操作难以验证安全性，还因为负责监听消息的服务器不在任何区块链系统内，只能通过监听到的消息和预设的消息格式来还原操作指令。这样一来，还原的准确

性依赖于发布消息、监听和解码这一系列过程的正确性，难以被验证。

另外，不同跨链项目的代码复杂性较高，差别也比较大，潜在的安全性问题也更为多样化。与仅存储于单一链上的资产相
比，跨链网络所涉及的资产更不稳定，也更易丢失。

跨链桥之所以复杂，是由于跨链双方是完全不同的系统，跨链网络作为中间第三方，它的消息处理能力、消息验证发行的安全性等，都有潜在的风险。

尽管「桥」增加了资产转移过程中的安全风险，但跨链项目依旧大量涌现，活跃在「桥」上的资金就像静置盘中的蛋糕，美味又易取，吸引黑客前赴后继来下刀。

Ronin Bridge
被黑给项目方们又上了一课：
想避免黑客攻击事件发
生，最重要的是保证私钥的安全性。
在具体执行上，可以使用安全性更高的硬件钱包；保证多个私钥的分散性；及时撤销某个废弃节点的权限。

Web 3 的外衣，Web 2 的灵魂？

在人们的想象中，「去中心化」的区块链和 Web 3
世界，安全性是与生俱来的特性之一。没想到它却是不成问题的问题。

这是多个因素博弈的结果，也是一笔
经济账。
在设计上，跨链桥可以实现去中心化，也可以中心化，但去中心化的设计成本和运行成本都高于中心化，因为它更加复杂。

如前文所说，在去中心化的桥上转移资产，需要获得多个节点的签名，依赖复杂的设计和资源投入才能实现。如果换成中心化的桥，项目方的设计和管理都更加方便，成本更低。
一些跨链项目为了系统的高效和便捷，采取了中心化的信息处理方式。

有观点认为中心化的桥偏离了 Web 3 的精神，背后还是一套 Web 2 的旧逻辑。

但在王沛宇看来，目前跨链桥的存在还是更接近 Web 3，属于典型的 Web 3
产物。
因为跨链桥的功能就是把钱从一个区块链转到另外一个区块链，这是在桥上实现的

。几乎所有的桥的实现都包含了智能合约的逻辑，智能合约是存在于区块链上的代码。

中心化和去中心化的界限并不是泾渭分明的，Web 3
的世界存在着「中心化风险」。

黑客入侵事件频繁发生，
一个原因是智能合约在编写时埋下了安全漏洞，另一个原因是 DeFi
项目在设计时存在逻辑漏洞，
例如没考虑到加入手续费可能会对交易逻辑产生的影响。

对于 DeFi
来说，
「中心化风险」通常源自某个
项目中存在特权账户。
特权账户可以随意更改智能合约的配置，甚至动用其他普通用户的资金，存在转移资金的风险。

当特权账户在更新配置时出现操作失误，也会给其他用户造成损失。

特权账户手
里的权力过大，还可能
为黑客提供一张自由进出的通行证。
一旦黑客攻下了特权账户的私钥，就可能通过这个账户盗取项目资金，损害其他人的权益。

跨链技术和项目的诞生，打通了加密世界不同区块链之间的壁垒，可以提高虚拟货币的经济流通性。以 Axie 为代表的 GameFi
产品，丰富了区块链的应用场景，让技术更加亲民，降低了 Web 3 的参与门槛。

但值得警惕的是，没有一成不变的美好。正如现实世界一样，有利益的地方往往潜藏着危机，利益越大，危机越复杂。

Ronin Bridge 被黑确实给埃文斯这样的氪金玩家提了个醒，但他并不打算放弃这个游戏。「我依然相信 Axie，我热爱这个社区里的一切。」

参考资料：

https://www.nbcnews.com/tech/crypto/axie-infinity-hack-leaves-players-

shaken-still-loyal-rcna23379

https://www.theverge.com/23017107/crypto-billion-dollar-bridge-hack-decentralized-finance

https://blog.chainalysis.com/reports/2022-defi-hacks/