



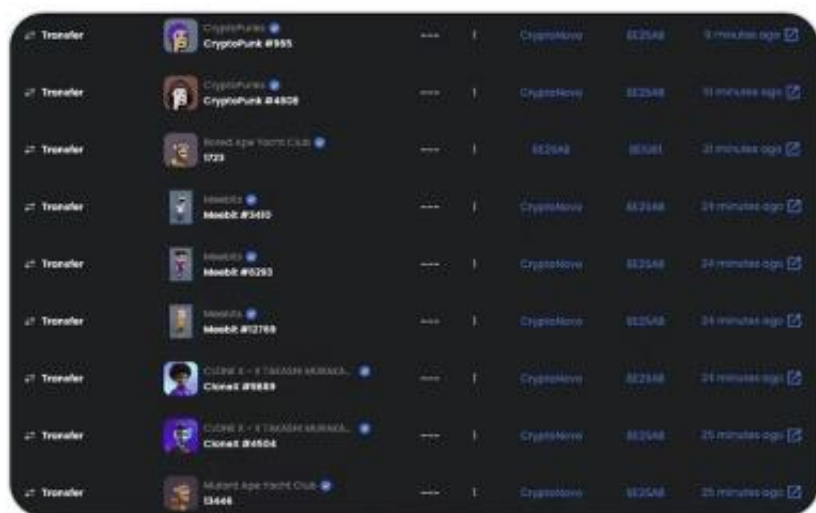
Cirrus   
@CirrusNFT



Massive hack including a Hoodie punk, a BAYC and some grail meebits just went down

Something like 600E worth of assets gone in a flash :(

[翻译推文](#)



下午12:02 · 2023年1月4日

独立国际策略研究员陈佳向《华夏时报》记者表示，欧美数字资产市场中的区块链技术安全事件实际上从来都没有得到系统性解决，反而在近期因币圈估值系统性崩盘而加速“内卷”，导致本就羸弱的安全性基础设施建设更加捉襟见肘。

2022年，比特币褪去了光环。加密分析公司Arcane Research发布《2022年终报告》显示，2022年比特币收盘下跌65%，仅次于2018年73%的跌幅，是自2011年以来第二糟糕的年度表现，ETH创下了69%的跌幅，而黄金仅下跌1%。

在比特币等加密资产价格持续走低的同时，也沦为了黑客们的“天堂”。据欧科云链研究院不完全统计，2022年前11个月区块链生态攻击发生275起安全事件，较2021年同期增加了30%，造成总计约27.69亿美元的损失，折合人民币近200亿。

“当市场陷入衰退风险的大环境下，数字资产的技术安全性并不会因为区块链技术日渐成熟而形成优势，反而是因为行业内卷人力资源投入不足和黑客盗窃需求增加而陷入更为严峻的困境。”陈佳如是说。

在陈佳看来，在币圈深陷衰退、行业企业内卷的大环境下，作为区块链技术金融应用的数字资产安全性风险反而越来越高。如此频繁的出现区块链技术安全事件绝不是偶然的，它有着非常明显而深刻的顶层设计和技术发展的原因。

“这些层出不穷的黑客攻击和骗局正导致一些用户在沮丧和恐惧中离开，也让外界更多质疑Web3的安全性。我们当然希望用户对自己的资产负责，但在很多专业攻击者面前，个人有时会显得无力，这时我们需要更多专业的Web3安全机构来为整个行业保驾护航。”欧科云链研究院高级研究员蒋照生向《华夏时报》记者表示。

蒋照生表示，一系列安全事件和暴雷事件的发生，正催生更强有力的加密监管。尽管我们不愿意看到过度监管抑制创新的发生，但随着监管机构对虚拟资产领域的了解愈发深入，野蛮生长的时代正在终结，全球监管态势已不可避免。对于加密世界的机构而言，监管重要性正进一步凸显，拥抱合规将成为行业良性发展的必选项。

记者了解到，除黑客攻击外，加密资产还被频繁的用于欺诈骗局当中。中国人民银行支付结算司发布的数据显示，2021年涉诈款项的支付方式中，利用加密货币进行支付仅次于银行转账，排名第二，高达7.5亿美元；而2020年、2019年仅为1.3亿美元、0.3亿美元，逐年大幅增长的趋势明显。值得关注的是，加密货币转账在“杀猪盘”诈骗中增长迅速。2021年“杀猪盘”诈骗资金中1.39亿美元使用加密货币支付，是2020年的5倍、2019年的25倍。

上海瀛泰（临港新片区）律师事务所主任翁冠星律师向《华夏时报》记者表示，从法律上而言，目前其实并没有一部法律法规非常完整地来规制链上安全的问题。因此，除了直接盗取“密钥”“私钥”或通过技术手段暴力破解这些密钥，其他的一些所谓“攻击”手段，有可能都不是一个“违法行为”，这对于整个市场来说都不是一个健康的态度。因此通过立法对于整个链上的交易作出统一的认定和规制是十分必要的。

## DeFi与跨链桥成重灾区

数字资产领域研究机构TheBlockRes发布的报告显示，2022年，从DeFi漏洞中窃取的资金总额达到20亿美元，同比增长48%。同时，在2022年10个最大的漏洞中，有6个是与跨链桥相关的，因为跨链活动越来越多。

“2019年的时候，大多数黑客攻击的目标都是中心化交易所。但是现在，绝大多数

的攻击都集中在去中心化金融 ( DeFi ) 协议。在DeFi内 ‘代码即法律’ 。如果智能合约中存在漏洞，那么黑客就可以利用它，让自己获利。”一位链上安全技术人员向《华夏时报》记者表示。

OKLink监测数据也显示，DeFi、社交媒体、跨链桥和NFT相关项目在2022年更易遭受攻击，约92%的安全事件都发生在这四大领域。在损失金额方面，2022年前11个月，超过80%的安全事件损失都集中在DeFi和跨链桥领域。

对此，陈佳表示，作为以去中心化为基石目标的数字资产交易平台，其借贷、储蓄和兑换等金融产品和服务中大幅去除了中间商，减少了交易费用，极大的提高了交易效率。然而，DeFi的高回报的另一面则是高风险，智能合约的开放性让代码漏洞不可避免。而在DeFi圈中有能力且有意愿发现和利用这些漏洞的技术人员数量不少。这就造成DeFi安全性敌我双方力量严重失衡，且缺乏纠正机制。

“由于数字资产行业特殊性，真实的损失统计数据被严重低估了。黑客入侵的教训并没有真正得到重视，黑客事件依然是目前困扰DeFi正常发展的最大桎梏。”陈佳表示。

萨摩耶云科技集团首席经济学家郑磊也向《华夏时报》记者表示，DeFi属于数字金融但无法监管，具有传统金融不具备的技术风险，必须开发既符合非中心化特征，又能进行实时有效监管的数字技术和监管体系，这是短期无法实现的目标，DeFi上的数字资产无法保证安全。

当前，数字资产安全如何保障是摆在区块链技术人员面前最具挑战性的问题。在陈佳看来，如果只是单方面把责任推给广大普通投资者是非常不合理的，无法弥补DeFi等数字资产在机制设计上的缺陷。同时，目前很多投资人对链圈币圈的理解知之甚少，只是一味盯着营销广告的高回报率，在区块链技术安全与投资者理性方面的教育均处在缺位状态。

“保障数字资产安全，就需要把 ‘安全基因’ 深度植入到全生命周期中。”数字化领域专家、农文旅产业振兴研究院常务副院长袁帅向《华夏时报》记者表示。

袁帅表示，从用户角度来看，目前数字资产市场还处于野蛮生长阶段，尚没有针对的监管机构对其监管和规范，所以更多的时候需要持有者强化自身的防护意识，保证自己财产的安全性防患于未然。用户不应把资产全部放在一个钱包中，分散来放是最能提高防盗安全性的方法。同时，应定期清理权限授予能够从一定程度上降低风险。此外，还应注意分辨真假，关注官方信息，杜绝投机心理，选择一个安全正规的良好平台。