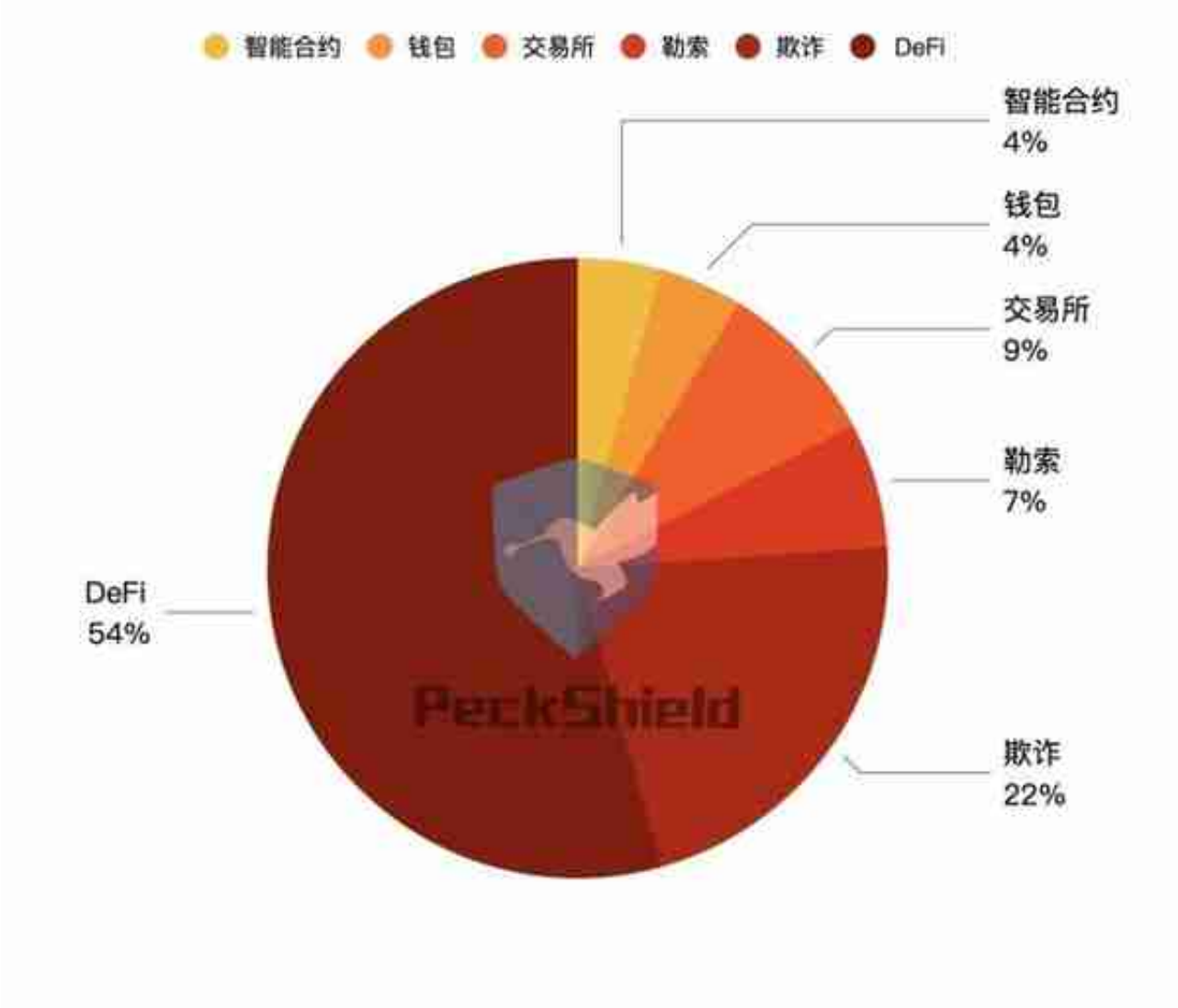
据 PeckShield 态势感知平台数据显示，过去一个月，整个区块链生态共生 46 起较为突出的安全事件。涉及 DeFi 相关 25 起、交易所相关 4 起、勒索相关 3 起，欺诈事件 10 起，钱包相关 2 起，智能合约相关 2 起。



据 PeckShield 「派盾」统计数据显示，2021 年 5 月共计发生 23 起与 DeFi 相关的安全事件，损失金额约 2.8 亿美元，其中，闪电贷攻击约 11 起，在 BSC 链上发生的与 DeFi 相关的安全事件 15 起，在以太坊链上的 3 起，在 EOS 上的 1 起。

闪电贷攻击频现，从去年的以太坊转移到了今年大热的 BSC 上，不少人将“闪电贷”解读为“作恶的源头”“建立在 DeFi 之上的核弹”“攻击者空手套白狼的本金”。

实际上，这些言论是对闪电贷的误读，闪电贷只是利用区块链技术，将传统借贷市场无法实现的事情带来一种新的可能。理论上，闪电贷借贷允许用户通过无抵押的方式借出流动性池内的所有通证，并要求用户在进行一系列互换抵押清算操作之后、交易结束之前归还所借通证以及固定的借贷成本。

在 BSC 首次出现的闪电贷攻击是 5 月 2 日，PeckShield「派盾」通过追踪和分析发现，DeFi 协议 Spartan Potocol遭到闪电贷攻击。之后闪电贷攻击出现在 BSC 链上的频率呈上升趋势，包括PancakeBunny、Bogged Finance、AutoShark、BurgerSwap、JulSwap。

PeckShield「派盾」观察发现，这些闪电贷攻击手法与以太坊上曾出现的闪电贷攻击大同小异，只是从以太坊转移到 BSC。随着年初 BSC 凭借低手续费、出块速度快等优势吸引了一批原以太坊上的 DeFi 协议和 Fork 以太坊上的 DeFi 协议，DeFi 的生态日益丰富，绑定在 BSC

上的资产也越来越多，这也使其成为攻击者睥睨的「收割场」。

从上述 6 个闪电贷攻击案例中，我们发现大部分攻击与之前发生在以太坊上的攻击十分相似。

BurgerSwap 与 OUSD 的攻击手法有异曲同工之妙。基于 BSC 的 BurgerSwap 和基于以太坊上 OUSD的闪电贷+重入攻击有相似之处，攻击者都是先从提供闪电兑换的去中心化交易所借出一笔闪电贷，再在智能合约中存入假币和原生 Token（BURGER、OUSD），并在此步骤通过重入攻击来攻击合约，最后归还闪电贷完成攻击。

操纵 CurveyPool 的闪电贷攻击在 BSC 上重现。5 月 30 日，BSC 链上结合多策略收益优化的 AMM 协议 Belt Finance 遭到闪电贷攻击，PeckShield「派盾」通过追踪和分析发现，此次攻击源于攻击者通过重复买入卖出 BUSD，利用 bEllipsisBUSD 策略余额计算中的漏洞操纵 beltBUSD 的价格进行获利。

值得注意的是，Ellipsis 是以太坊上 DeFi 协议 Curve 授权 Fork 的项目，多次操纵 Curve yPool 的价格，以套取稳定币价差的套利事件重现，Fork Curve 的潘多拉魔盒是否已经打开？

综上，这些重现的闪电贷攻击都有迹可循，并非没有防御的办法。

PeckShield 「派盾」相关安全负责人表示：“协议开发者不仅要读懂 Fork 的 DeFi 协议，还要读懂自己的协议，协议的乐高性不是简单的拼接，而是在完全理解原协议背后的逻辑进行组合。目前对于闪电贷攻击并非没有解决的办法。我们发现攻击者多从已知的漏洞下手，要做的就是在协议上线前做好静态审计，排除已知的漏洞；当其他协议遭到攻击时，自查代码，排除同源漏洞；研究以往的案例，定期做动态审计，避免漏洞重现。除了寻求专业代码审计团队的帮助，还需引入第三方安全公司的威胁感知情报和数据态势情报服务，完善防御系统。在攻击发生时，确保第一时间感知并及时采取应对措施。”