在本周&#039；s比特币技术周刊，我们将重点关注一个影响闪电网络支付的安全问题。随着比特币链条中交易成本的增加，其安全风险也会暴露出来，但目前的解决方案仍存在较大的取舍。。然后，我们将介绍一个新的预签名保险库提案，最后，一般内容，如流行的Q&amp比特币StackExchange和流行的比特币基础设施的重大更新。

闪电网络遭遇新的安全问题，短期解决方案可能不尽如人意

本周，来自SquareCrypto的闪电网络开发者MattCorallo公布了一种窃取闪电网络(LN)节点资金的新方法。。这个问题与现有的一个众所周知的费用管理问题部分重叠，但据我们所知，这个漏洞并没有被利用，因为在过去的两年中，几乎所有链上的中继交易都可以相对快速地得到确认，即使他们只支付默认的最低中继费率。

但是，如果在很长一段时间内费率大幅增加，这些问题将变得更加严重。如果您担心此问题可能会影响您的渠道，请联系闪电网络软件开发商。

我们将详细解释这个问题：

闪电网络(LN)支付原子性的新攻击：MattCorallo在闪电网络开发邮件列表和比特币开发邮件列表中同时发帖，披露了讨论中发现的一个新攻击。它允许LN承诺交易通过锚输出增加CPFP(父子支付)费用。我们将通过一个例子来描述这种攻击：Alice使用LN通道给Bob发送一个哈希时间锁定契约(HTLC)。合同旨在通过以下任何一种方式解决：

如果Bob公开了前像，他可以花Alice&#039S1BTC；

否则，80块后。爱丽丝可以把这1BTC拿回来；

Alice还告诉Bob，她的目标是向Mallory付款，因此Bob使用他与Mallory拥有的频道向她发送相关的HTLC:

。

如果马洛里公开了原始图像，她可以花鲍勃&#039；s1BTC(在这个例子中，我们忽略路由费用)；

否则，40个街区后，鲍勃可以把这1个BTC拿回来；

虽然上述HTLC通常是在链外创建和结算的，但各方也有一个承诺事务，可用于将HTLC承诺放在链上。单笔连锁结算交易可以满足HTLC的任何条件。

例如，Mallory可以发布已提交的事务。，然后创建一个结算交易，提供原始图像并索赔鲍勃1BTC。如果鲍勃在第80块爱丽丝之前看到马洛里的原始图像-鲍勃&#039；的合同超时，Bob可以提取原始图像。并用它从爱丽丝那里得到1BTC(链上或链下)。

或者，如果鲍勃没有&#039；如果看不到原始结算交易，Bob可以在40个街区后创建自己的退款结算交易，以收回他的1BTC。这样，他也可以发起爱丽丝&#039；s 1BTC退款(也可以是上链或下链)。不管是哪种情况，这都会让大家遵守自己的契约意图。不幸的是，正如马特科拉洛本周透露的。马洛里似乎有办法绕过这个过程。她可以阻止Bob学习原始图像，并阻止他发送退款结算交易。

原始图像拒绝：Mallory可以通过给她的原始图像较低的费用比率来结算交易，从而避免其快速确认，从而防止Bob了解原始图像。如果鲍勃只是在区块链寻找原始图像，那么在没有确认的情况下，他赢了&#039；见不到马洛里&#039；一言为定。

退款拒绝：由于这两个交易之间的冲突(意味着它们都使用相同的输入)，Mallory先前广播了原始图像来结算交易。，可以阻止矿工和比特币中继节点接受Bob稍后广播的退款结算交易。理论上，鲍勃&#039；退款结算交易可以取代马洛里&#039；的原始结算交易支付更高的费用，但事实上，Mallory可以使用各种事务锁定技术来防止这种替换。因为鲍勃可以&#039；他不知道最初的结算交易，他不能&#039；无法确认他的退款结算交易。因此，一旦经过了80个街区，爱丽丝就可以收回她在《爱丽丝-鲍勃HTLC》中提供给鲍勃的1BTC。当马洛里&#039；的原始结算交易最终确认马洛里在《鲍勃-
马洛里HTLC》中得到了鲍勃提供的1BTC，使鲍勃失去了1BTC。

MattCorallo在他的文章中考虑了几种解决方案。但是它们都遇到一些问题或者涉及到重大的取舍：

需要一个存储池：Bob可以使用一个比特币全节点来监控比特币P2P中继网络，了解Mallory的结算交易。。一些LN节点(如艾克蕾尔)已经这样做了，这似乎是一个合理的额外负担，因为该问题只直接影响路由节点(如鲍勃)。

仅代表自己发送或接收付款的节点只会受到间接影响。因此，日常用户仍然可以在移动设备上运行轻量级LN客户端。不幸的是，并非所有节点都像其他节点一样接收相同的事务，即使所有节点都工作良好。更糟糕的是，像Mallory这样的攻击者可

以使用一些技术向不同的对等方发送不同的冲突事务(例如，向已知的矿工发送固定的原始结算事务，但是向非矿工中继节点发送具有至少一个相同输入的不同的非结算事务)。

中继网络可以向事务提交者(如Bob)提供有关冲突的信息，所以它们不会&#039；不需要经常监控自己。仍然会有坏参与者的问题，比如Mallory使用targetrelay向矿工和非矿工发送不同的事务。此外Bob也可以支付矿工或者其他第三方节点，但是需要一些人运行额外的软件，部署LN协议升级可能没那么容易。

结算交易锚点输出：您可以重新设计链上的结算交易，并将其值用于锚点输出。，这些产出可能是利用CPFP的瓜分和增加CPFP(父子付款)的费用。这将要求这些交易变得更大(增加链成本)并被预先签署(降低灵活性)。

这只会直接影响到那些在等待付费的时候单方面关闭的渠道，这已经是一种可以显著增加链条上成本的情况，所以用户都在尽量避免。然而，增加链上的执行成本也增加了支付可以通过LN不受信任地发送的最小真实值。。尽管存在这些挑战，但在撰写本文时，这似乎是最理想的解决方案。

Corallo称这是一个严重的问题，但他也指出，这个问题的后果类似于另一个关于链上LN交易中成本管理的已知问题。

到目前为止，我们还没有&#039；t发现实际的LN损失是由于链上费用管理的问题造成的，这可能部分是因为在过去的两年中，很少有持续时间足够长的大规模费用高峰。

但是这种好运气可以&#039；不要无限期地持续下去。因此，这一新问题给了LN开发者一个额外的理由来优先改善链上成本管理的实施。在此期间，关注攻击的节点运营商可能希望增加其cltv_expiry_delta，以便使原始结算交易有更多的确认时间。

在当前LN节点中，C-Lightning的默认值为14。LND的默认值是40。锈闪电的默认值是72。艾克蕾尔的默认值是144。请注意。增加该值将使您的渠道不太受用户欢迎，因为较高的值可能会延迟付款。

新的多方保险库合同实现

基于上周提到的预先签署的保险库合同原型&#039；周报。Antoine“darosior”poinsot宣布了一个名为Revault的演示实现。这种新的实现侧重于使用多重签名安全性存储多方共享资金。。该协议允许一部分参与者通过确认信标交易来启动撤销

过程。

如果保险库中的其他方反对取款，他们有机会广播第二笔交易，并将资金返回到保险库中的紧急地址。。如果在一定时间内没有异议，另一笔交易就可以完成资金的提取。Poinsot目前正在寻求对该提案的反馈。

StackExchange精彩问答

比特币StackExchange是Optech投稿人寻找问题答案的首选。这一期，我们将重点介绍一些最近最热门的问题和答案。

问题1:如果我们使用原始公钥作为地址，对ECDSA的潜在攻击是什么？

PieterWuille总结了在地址中使用公钥hash代替公钥可以减缓量子计算攻击的论点。。他接着列出了为什么声称的论点可能被夸大，并给人一种虚假的安全感的原因。

问题2:子代付款中DEFAULT_ANCESTOR_LIMIT对于父代是什么意思？

Murch指出，这种默认策略有助于防止垃圾邮件攻击。，并提供了一些确定祖先事务计数的示例。

问题3:与脚本语言相比，简单性如何更好地适合静态分析？

拉塞尔奥&#039；《简单性白皮书》作者康纳描述了比特币脚本静态分析相对于简单性语言所面临的挑战。

比特币主要基础设施发布候选更新

比特币核心0.20.0rc1是下一版本比特币核心软件的首个发布候选；

LND0.10.0-betarc6允许测试lnd客户端的下一个主要版本。

C-Lightning0.8.2-RC3是下一版本C-Lightning客户端的最新候选；

除了这些，本周比特币核心发生了一些重大变化。(注：下面提到的比特币核心的变化要到0.21版本才能看到，即将到来的0.20版本不会加入这些新功能。).

比特币核心#15761增加了upgradewalletRPC，允许用户在加载钱包时解锁钱包，

并将其升级为分层确定性(HD)钱包。这一附加功能也与多个钱包兼容。

比特币核心#17509允许钱包GUI将部分签名的比特币交易(PSBT)保存到文件中，并从文件中加载PSBT。后续的公关预计将增加的能力，签署PSBT在图形用户界面。