1. 问：什么是闪电网络？

答：闪电网是一个去中心化的网络，旨在实现比特币所有权的实时离线转移，不需要可信的第三方。该系统仍在开发中。(译者&#039；s注：原文写于2016)

闪电网络使用由多个地址组成的双向支付通道。

打开和关闭通道都需要一个链上事务。

通道一旦开通，价值就可以在交易对手之间实时转移。交易对手相互发送比特币交易。，但它们不会被广播到比特币网络。

新事务将覆盖以前的事务。只要通道没有关闭，交易对手就会在本地存储所有数据。

2。问：闪电网是开源的吗？那&#039；这是对的。闪电网是开源的。任何人都可以审查闪电网的代码(就像审查比特币的代码一样)。

3。问：谁拥有闪电网络？受谁控制？

答：闪电网和比特币一样，不归任何人所有。，而且不受任何人控制。

闪电网的代码是开源的，任何人都可以下载查看。

任何人都可以运行节点并加入网络。

4。问：闪电网络的创建者是谁？

答：JosephPoon和ThaddeusDryja撰写了一份关于闪电网络的白皮书。

闪电网络是一个开源项目，任何人都可以贡献代码。

目前，有几个独立的实现正在开发中：

lnd—LightningLabs

eclair—ACINQ

Lightning—d—blockstream

5。问：闪电网络自己发行代币吗？答：不，没有必要这样做。

闪电网将使用真实的比特币进行交易。

6。问：闪电网的实现是否依赖共识？

答：不需要，闪电网的实现不需要比特币网的共识。

闪电网既不是软叉，也不是硬叉，而是在比特币网的基础上构建的附加层。

因此，雷电网络的实现不需要共识。

7。问：闪电网络是否存在托管风险？我需要将我的资产交由其他可信方保管吗？

答：不是，闪电网不是基于信任。你的资产仍然完全在你的控制之下。

如有问题，你只需要像普通的比特币交易一样，向链上广播渠道的最新状态。

你所有的资金都会返还到你的比特币地址，并记录在链上。

8。问：我听说闪电网上交易发生在链下.这是否意味着我的比特币将被从链上抹去？

答：不会，你的比特币永远不会离开区块链。

当您的支付通道打开时。，您的比特币将被存储在一个多签名地址中。通道关闭后，最后一笔交易会上线。

&quot；链下&quot不是一个非常恰当的表达。之所以用它，是为了强调所有权转移不再体现在链条上。

9。问：听说闪电网络要锁定我的比特币.这是真的吗？

答：就闪电网而言，这个词&quot锁仓库&quot是极具误导性的。

闪电网络不会影响您访问自己的资产。

实际上，闪电网络频道将使您的资产更易于使用。

首先，在闪电网，你不&#039；不需要等待确认，资产的转移几乎是瞬间的。

其次，让你的资产回到链条上，就像发送普通的比特币交易一样简单。。您只需等待确认，您的资产将从&quot离线&quot到链条上。

只有一种例外：你的通道在交易过程中出现故障(交易对手离线)，但这种情况很少见。

出现上述异常时。你必须等待一段时间才能使用你的资产。等待时间取决于你的支付通道的参数(估计最短几个小时，最长几天)。

10。问：闪电网络有自己的区块链吗？

答：没有闪电网络依赖于比特币区块链。比特币网络中的对等节点在开启和关闭支付通道时，需要执行链上交易。

通道一旦打开，比特币的所有权可以在链下双向转移。

通道中的交易是正版比特币交易，但是当通道开放时，这些交易不会在比特币网络中广播，而是由通道中的交易对手存储在本地。

因此，闪电网可以实现实时交易和近乎无限的吞吐量。

11。问：有没有什么形式的挖掘来保证雷电网的安全？

答：不是，安全性是由比特币网络中的矿工提供的。

12。问：比特币区块链的计算能力高达2exahash/s但是闪电网没有计算能力来保证其安全性.闪电网怎么可能像比特币区块链一样安全？

答：闪电网的安全性来自比特币区块链。

雷电网不能独立运行。它完全依靠比特币区块链来确保安全。

简单来说，比特币网络就是闪电网下的安全网。

如果雷电网的通道出现问题(如交易对手断线)，也可以选择落入安全网。

(可以像普通比特币交易一样，向链上广播渠道的最新状态。)

13。问：闪电网络是否有自己的公共账本或数据库用于所有交易？

答：没有，闪电网没有自己的账本和数据库。

在闪电网络上持有价值意味着你有一个双重签名的交易。这些交易是有效的，但它们不会在比特币网络上广播。

您持有的交易属于2/2多重签名交易。

您和您的交易对手都将签署这些交易并将其存储在本地。

这些交易将使用多重签名地址作为输入(资金地址)，并指向两个不同的地址作为输出。

输出指向只有您可以控制的地址。另一个输出指向一个只有你的对手才能控制的地址。

14。(1)问：你说闪电网的所有交易都是真实的比特币交易.既然链上没有记录，怎么能说是真正的比特币交易呢？

简答：

要理解这一点，首先要明白什么是真正的比特币交易.

其实没有所谓的&quot代币&quot关于比特币区块链.仅向区块链提交签名的消息和更新。

假设爱丽丝给鲍勃发了一张1BTC.

我们称之为点对点交易，因为价值的所有权直接从Alice转移到Bob。

但是鲍勃没有。实际上没有收到&quot数字令牌&quot爱丽丝送的。

实际情况是，网络中的所有节点都将更新其本地存储的公共分类帐副本。

公共账簿更新后，&quot令牌&quot最初注册在爱丽丝&#039；的地址被重新注册在鲍勃&#039；的地址。

详细解释：

爱丽丝发给鲍勃的比特币交易，其实只是爱丽丝广播给大家的一条签名消息。

此消息不仅发送给Bob，还广播给网络中的所有节点。

撰写本文时。有5400多个&quot完整节点&quot在比特币网络中。

爱丽丝向鲍勃发送比特币交易的具体流程如下：

当爱丽丝广播一条她已经签名的消息(即比特币交易)时，该消息将被网络中的一些完整节点接收。这些所有节点将根据共识规则独立地验证消息(交易)。如果该节点发现该消息是有效的，它将再次向网络中的其他节点广播该消息。网络中的其他节点在接收到消息后重复上述过程。直到全网5400多个节点独立验证并广播消息(事务)。在某个时刻，矿工们成功地挖出了含有爱丽丝&#039；新闻(交易)。因为采矿要消耗大量的电力，矿工要承担高昂的成本。。矿工广播新挖的区块。一些完整节点将接收该块，并独立验证该块及其所有内容。这意味着他们将验证爱丽丝&#039；的消息(事务)两次。如果整个节点(根据共识规则)确认该消息是有效的它们将向其他完整节点广播该块。其他完整节点接收、验证并广播该块。该过程将继续，直到网络中的所有节点都验证了该块并验证了Alice&#039第二次报文(交易)。

从以上步骤可以看出。一个普通的比特币交易，实际上涉及到全网的参与者。爱丽丝&#039；s消息已经被5400个节点独立验证两次(共10800次)。尽管如此，我们仍然称它为&quot对等交易&quot因为价值的所有权直接从爱丽丝转移到鲍勃身上。然而，每个人都应该帮助更新他们本地的书籍。）

结论：

比特币交易本质上是签名消息。

假设Alice想通过闪电网上的支付通道给Bob发送1个BTC:

Alice在2/2多签地址存储了一些BTC，

Alice和Bob签署了相同的消息，将1BTC的所有权从Alice转移到Bob。

此消息为有效的比特币交易，但不会在比特币网络上广播。

Alice和Bob都在本地存储事务(消息)。

来自Bob&#039s的观点，这&quot双重签名邮件&quot值1BTC。

这条消息值1BTC的原因。因为Bob可以随时花掉链上的钱，只要把消息广播到比特币网络就可以了。

比特币交易=签名消息=闪电网上的交易

任何货币交易的目的都是为了改变价值的归属。

在比特币网络中，我们使用签名消息来改变价值的所有权。

闪电网络交易是双签名消息。

因此，双签名消息是真正的比特币交易。

14。(2)问：一个标准的比特币交易需要链条确认.宣称闪电在线交易和比特币交易一样公平真的公平吗？答：在这一点上，它们是不同的.[XY002][XY001]闪电网上交易是零确认交易。但是只要在比特币网络上播出，就和&quotchain&quot零确认交易。

只要支付足够的交易费用，这两笔交易最终都会被记录在比特币区块链上。

但是，与标准的零确认交易相比，闪电网交易采用不同的安全模式，所以可靠很多。

Lightning网络交易由工作负载证书间接保护。这是因为闪电网络完全依赖于底层的比特币网络(见问题12)。

在一个开放的雷电网络通道中。将会有一套不同的博弈论机制来提供不同类型的安全模型。

闪电网将在不引入可信第三方的情况下，扩展比特币的功能。

但代价是，你必须通过运行所有节点来监控比特币网络。

监控可以外包给其他人，但在这种情况下，您必须相信外部服务器会忠于职守。您的资产不会通过外部服务器路由。服务器的唯一功能是监控比特币网络和广播&quot罚款交易&quot必要时。

请注意。外包监控服务只是一种选择，你可以在没有的时候选择&#039；我不想运行自己的完整节点，并不是说你必须外包。

第三方不可能从闪电网的渠道盗取资金。还应注意的是，闪电网设计为小额(100美元以下)转账平台。

所有的闪电网络交易必须由渠道的双方参与者签字才能生效。所以传统的双支出攻击很难成功。

但是真正的风险是，攻击者可以向比特币网络广播过时的闪电网络交易。

过时闪电网交易是指代表非最新渠道状态的交易。

上述风险是您(或您信任的服务)必须运行Watcher节点的原因。

瞭望塔节点将监控广播到比特币网络的所有交易。

如果您的观察节点发现一个过时的事务，它将广播一个&quot罚款交易&quot作为回应。

惩罚交易赋予你没收你通道内所有资产的权利(包括原本属于你交易对手的资产)。

但是，您播报的处罚交易只有在您发现过时交易在线播报的情况下才会生效。

因为你可以广播处罚交易，所以你的交易对手在广播过时交易时需要承担很大的风险。

另一个安全/隐私功能是，所有闪电网络交易将在参与者之间进行端到端加密。

总结：

闪电网络交易在安全模式上不同于传统的比特币交易。

比特币网络一经播出，闪电在线交易将被视为有效的比特币交易。

但是，

只要支付通道打开，闪电网就不会广播，只会在通道内的参与者之间交换，并由参与者存储在本地。

因此，我们可以将闪电网交易定义为

非广播零确认多签名的比特币交易，并附加安全机制。

15。问：我听说闪电网络要求用户持续监控区块链.这是真的吗？

是的，它&#039；这是真的。

用户需要运行软件来主动监控区块链上是否存在违约行为(即广播过期交易)。

但是，用户也可以将监控外包给第三方服务提供商。

外包不会侵犯你的隐私，但是你一定要相信服务商是诚实可信的。

优点：

这将鼓励更多的人在比特币网络上运行整个节点。

你的整个节点甚至可以帮你赚点小钱：

&quot；所有节点/闪电网络节点&quot可以赚取手续费作为&quot鲍勃&quot(详见下文解释)。

您也可以选择自己配置整个节点，以提供区块链监控服务。理论上，这会给你带来一些&quot微薄收入&quot。

16。问：听说闪电网络会收取一些费用.这些费用是给谁的？

答：任何运行闪电网络节点的人。

例：

爱丽丝想给卡罗尔转账。但是爱丽丝和卡罗尔之间没有支付渠道。幸运的是，Alice和Carol都与Bob建立了支付渠道。Alice可以通过Bob将付款转给Carol。，避免与

Carol新开通道的麻烦：

Alice-

Bob-

Carol

这种情况下Bob会收取少量手续费。

17。问：使用路由支付时，如何防止中介Bob盗用？

简答：

鲍勃先用自己的钱付给卡罗尔，再从爱丽丝那里把钱拿回来。

详细解释：

Carol生成一个随机数r作为临时秘密值。Carol计算r的hash值h，Carol把h的事告诉Alice，Alice创建了一个特殊的转账交易，收款人是Bob。但是，事务必须包含r才有效。此时由于R不足，交易无效。Alice告诉Bob关于H的事情，Bob知道H是丢失的r的哈希值，Bob创建了另一个特殊的转账交易，收款人是Carol。。但是，该事务也必须包含r才有效。此时，因为Bob没有R，所以交易无效。卡罗尔想拿回她的钱，所以她把R的事告诉了鲍勃，让交易生效。因为Bob已经有了Alice创建的交易，，可以直接把r放入交易中使其生效。Bob可以根据R的hash值H来验证Carol是否给了他正确的R，同时Bob也向Alice透露了R。

现在爱丽丝可以用R来证明她已经付钱给卡罗尔(R充当收据)。

18。问：闪电网需要隔离见证吗？

答：可靠答案请戳

。19。问：在哪里可以找到更多关于闪电网络的信息？

答：雷电网相关信息：

以上是科普的详细内容：雷电网常见问题总结及解决方法。更多关于闪电网的常见问题，请关注dadaqq.coM其他相关文章(www.dadaqq.coM)！

本站提醒投资有风险，入市需谨慎。此内容不作为投资理财建议。