
         Understanding the Lightning Network, Part 3: Completing the Puzzle and Closing the Channel
        

闪电网络可能是部署在比特币之上最受期待的技术创新。支付层，约一年前由Joseph Poon和Tadge Dryja首次提出，保证比特币安全性的同时，以几乎免费的方式支持用户之间几乎无限数量的链下交易。

至少有三家公司——Poon和Dryja的[Lightning](http://lightning.network/)、[Blockstream](https://blockstream.com/lightning/)和[Blockchain](https://www.blockchain.com/api)——目前正在致力于该技术的实现。但在这个前沿技术普及之前，很少有人能完全理解小额支付将如何提升比特币的交易容量。

在这个由三部分组成的系列中，展示了闪电网络的基本组成部分，并展示了它们如何结合在一起以实现即将到来的协议层。

本系列的第一部分介绍了基本组成部分，并解释了如何使用这些基本组成部分建立双向支付通道。第二部分介绍了网络的形成过程，以及哈希时间锁（HTLC）如何将网络中的不同通道链接在一起。本系列的第三部分和最后一部分解释了如何将HTLC放置在双向支付通道中，以确保交易可以完全在链下发生。

闪电网络

到目前为止，Alice和Bob开通了一个双向支付通道，他们都抵押5个比特币。他们来回进行了两次交易，在当前的通道状态下，Alice和Bob都可以通过在区块链上“放弃通道”让自己领回5比特币。

现在，他们希望在通道中引入HTLC。这是为了让Carol向Bob索要比特币时Bob可以获得她的密语，那么Bob就同样得到了Alice的比特币。

和前面的步骤一样，Alice和Bob开始分别创建一个新的承诺交易来创建通道。包括一个普通的输出，一个输出到一个带有csv（checksequenceverify）时间锁和hash锁的新的多签地址。同样，和前面的步骤一样，Alice和Bob交换了他们的旧密语，以有效地使旧通道失效。而且，一旦交换，Alice和Bob都可以在承诺交易上签字，并随时将其放到区块链上。

这些和普通状态通道一样。除了一个变化，Alice和Bob的承诺交易现在都包括一个新的输出，价值一个比特币。（这使得余额为4-5-1；Alice为4，Bob为5，新输出为1。）

这个新的输出基本上是HTLC的输出。到目前为止，它比所有其他输出更有趣，因为有三种方法可以解锁它。

首先，新的输出（在Alice和Bob的承诺交易中）释放比特币，条件是Bob的签名和密语包含在后续交易中。因此，无论Alice或Bob是否签名和广播承诺交易，只有Bob可以解锁此输出（如果他确实有密语）。但是，这两个承诺事务之间有一个小的区别：如果Bob放弃了通道，那么会涉及到一个csv时间锁。他需要等1000个区块。（如果Alice放弃了通道，他可以立即领取比特币。）

如果Bob放弃这个通道，他必须等待1000个区块，这与我们以前看到的非常相似：它允许Alice拿走这个比特币，以防Bob试图签署和广播一个旧的通道状态。这就是第二种解锁输出的方法。如果Alice提供Bob的（最新的）密语，她可以“偷”钱。

如果Alice曾经试图欺骗和广播旧的状态到这个通道，Bob可以使用Alice的密语拿到这个比特币。（他甚至不需要提供密语。）

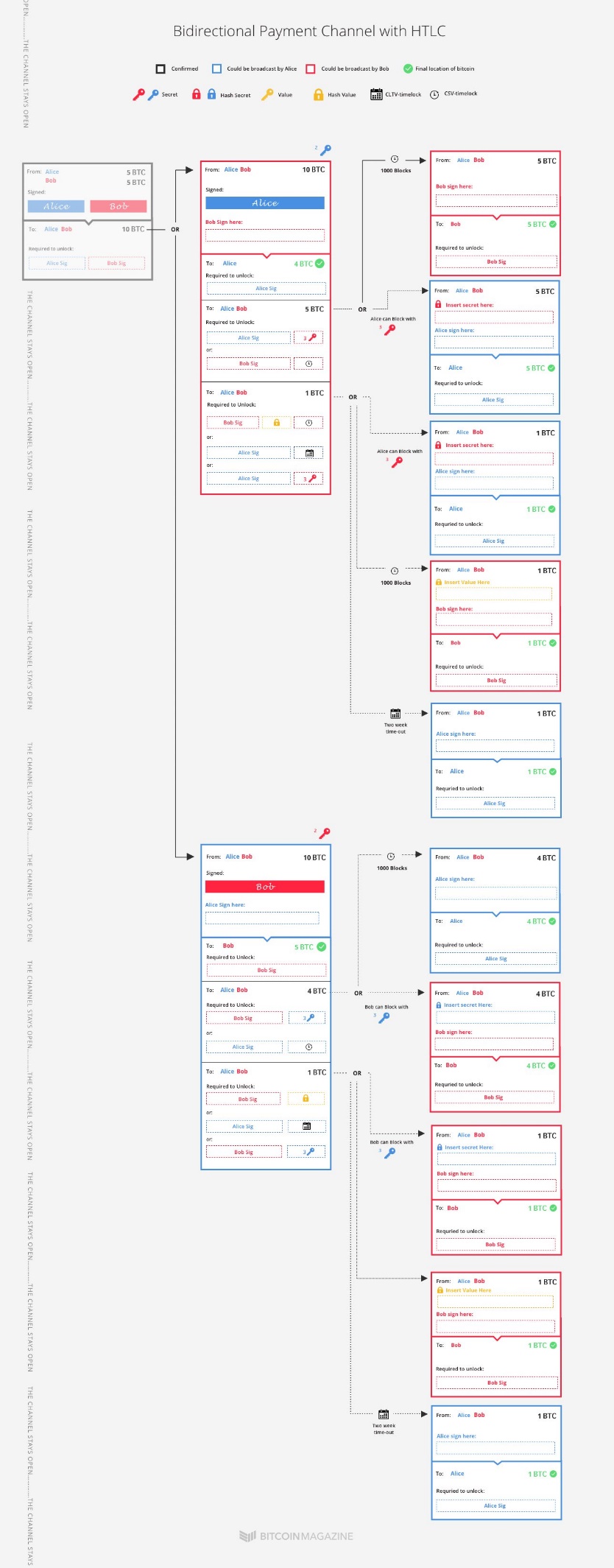
第三，与任何其他HTLC一样，这两项承诺交易也包括Alice通常的CLTV超时。如果Bob没有在一段时间内提供密语，比方说——两周内（例如，因为他没有从Carol那里得到），Alice就可以收回她的比特币。

那么

Alice和Bob都持有半有效的承诺交易。如果Alice放弃了区块链上的承诺交易，她会立即向Bob发送5比特币。此外，她还可以等1000个区块，自己要4比特币。另外，Bob有两周的时间提供密语，并在“HTLC输出”中申领比特币。（如果他两周内不提供密语，Alice可以申领该比特币。）

同时，Bob也可以随时放弃他的承诺交易，并立即向Alice发送4个比特币。然后，如果他提供了这个密语，他将等待1000个区块，从一个地址再申领5个比特币，从HTLC输出中申领另一个比特币。（如果他两周内不提供密语，Alice可以收回。）

当然，如果Alice或Bob在未来的任何时候试图欺骗，并且在这个通道上提交过时签名的状态，他们两个人都可以完全阻止另一个人窃取该通道中的所有比特币。



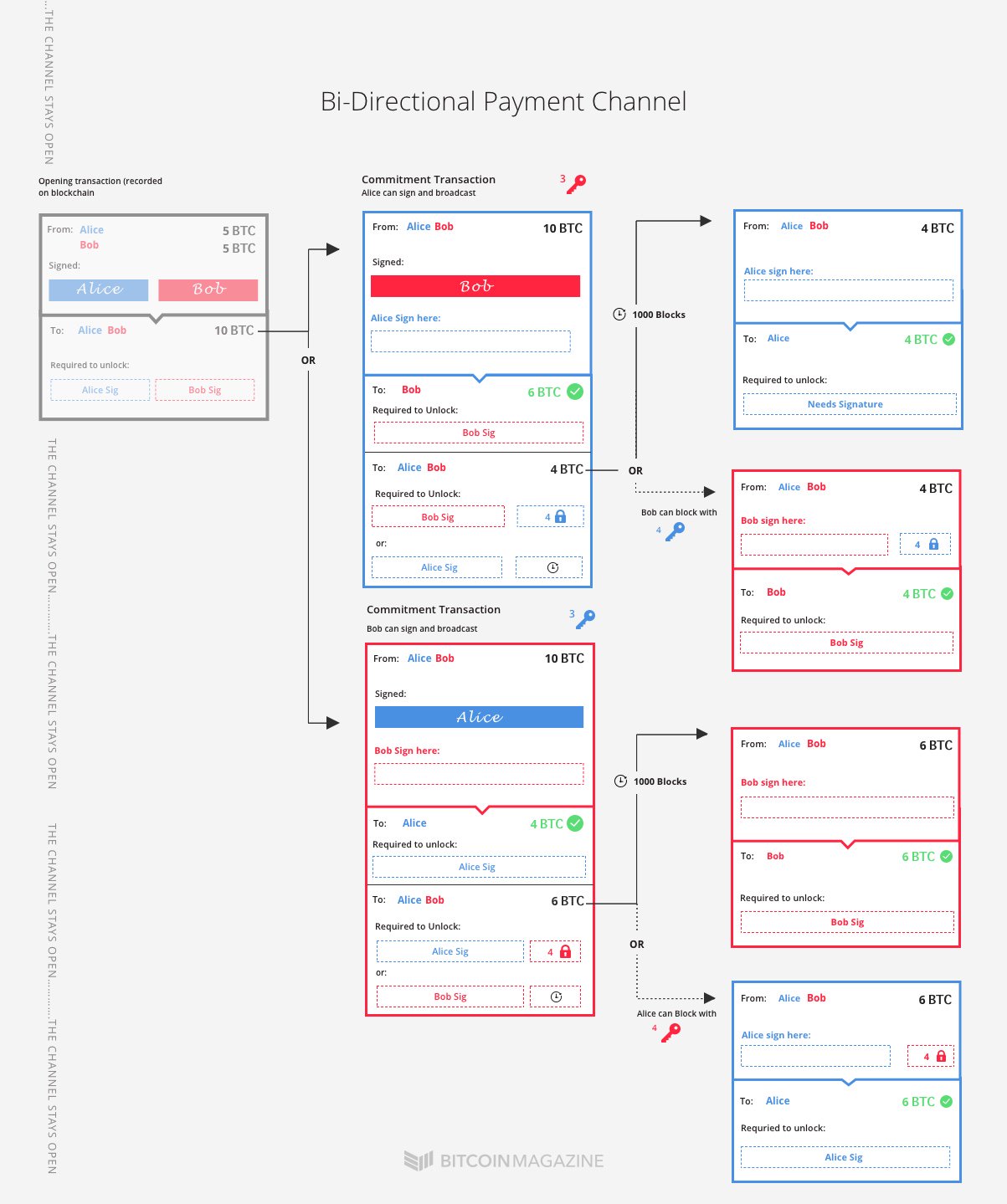
安装状态通道

Bob可以得到一个比特币（假设他有比特币）。但他必须广播和重新签名他从Alice那里得到的承诺交易，包括在随后的交易中的密语。

Alice知道这一点。她不可能窃取Bob的比特币，即使她通过其他途径发现了它的密语。

这两个状态通道可能还是在完全不同地理位置处开通的。Bob可以简单地将密语给Alice，Alice可以同意在没有HTLC和超时期限的情况下将通道状态更新为正常的状态。

假设双方都想保持通道打开，他们一般都会这么做的：这比将通道放到区块链上更容易。



关闭通道

最后，这里是闪电网络的最重要的：这三篇文章中描述的几乎所有内容通常都不需要比特币区块链。

如果Alice和Bob都想“和平地”关闭通道，他们只需创建一个交易来覆盖自期初交易以来发生的所有事情。在这个结束交易中，他们将通道中应该属于自己的份额发送给自己，以最新的通道状态为准。

具体来说，这意味着如果Alice想关闭通道，她可以在此时简单地创建一个交易，支付自己的4比特币和Bob 的6个比特币，并要求Bob签名和广播该交易。既然Bob没有理由不这么做，他很可能会合作，关闭通道。

最后，只有两个交易会通过比特币网络广播，并包含在一个区块中：期初和期末交易。即使Alice和Bob之间进行了100万次交易，这一点也成立，这将从比特币区块链中卸下了巨大的负担。

