了解闪电网络-第二部分-创建网络

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。

本系列的第一部分描述了必要的组成部分，并展示了如何将这些组成部分建立双向支付通道。第二部分说明双向支付通道是如何转变为网络的。

网络

在前一篇文章中，Alice和Bob建立了双向支付通道。现在，Alice想给第三个人Carol发送比特币。

为此，Alice和Carol可以在他们之间开辟一条支付通道。但实际上他们不需要。事实证明，Bob和Carol已经有了一个通道，所以Alice只需通过Bob支付Carol。

具体来说，Alice可以付给Bob一个比特币，而Bob可以付给Carol一个比特币。

然而，Alice并不真正信任Bob或Carol。她担心如果她付给Bob钱，Bob就永远不会真正付给Carol了。或许Bob会付钱给Carol，但Carol会说她从未收到过钱，Alice也不知道该怪谁。

因此，Alice想确保她付给Bob一个比特币，仅仅在Bob也付给Carol一个比特币之后。这是通过一个简单的密码技巧完成的。

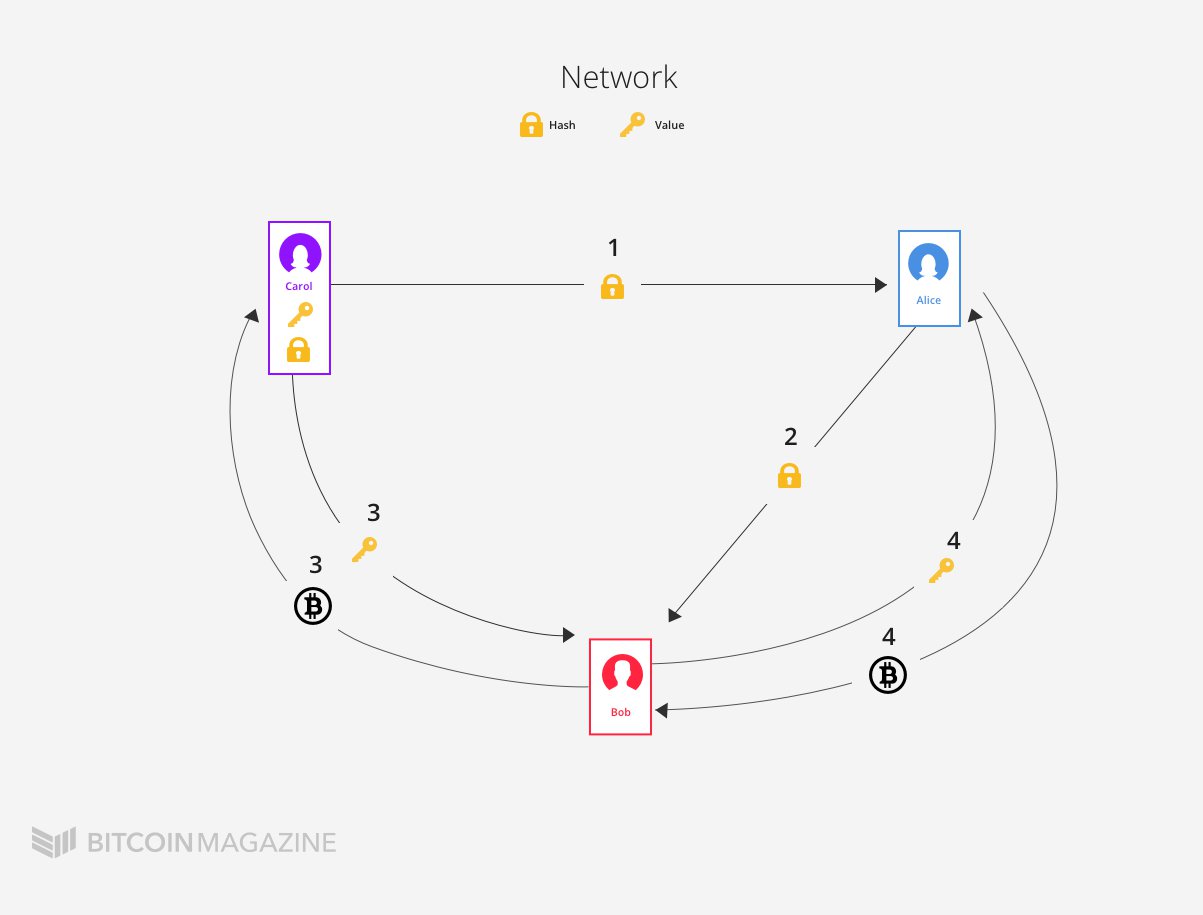
当Alice想给Carol发送一个比特币时，她告诉Carol创建一个密语（一个随机的数字串），然后把哈希值发给她。Alice还告诉Carol用比特币和Bob交换密语。

与此同时，Alice从Carol手中接过哈希值，转向Bob，告诉Bob，如果他能够提供哈希值相应的密语（只有Carol有），她会给他一个比特币。

于是，Bob转向Carol，给Carol一个比特币，Carol给Bob密语。

然后，Bob将密语发送给Alice。Alice知道Bob一定是从Carol那里得到了密语，以换取比特币，因此得出结论，Carol得到了她的比特币。所以Alice可以自信地给Bob一个比特币。

每个人都很高兴。



然而

在这种“简单”的情况下，中间人Bob仍然必须信任Alice和Carol。Bob在给Carol寄了一个比特币后，必须相信Carol真的会给他一个比特币，而Bob必须相信Alice，一旦他给了Carol一个比特币，Alice就真的会给他一个比特币。

但是，比特币的价值交易必须在网络上得到绝对保证。更具体地说：如果Bob给Carol一个比特币，他必须保证从Alice那里得到一个比特币。

这就是哈希时间锁（HTLC）出现的原因。

哈希时间锁HTLC

现在Alice和Bob现在需要使用HTLC来发送比特币。（Bob和Carol也采用同样的方式来发送比特币）

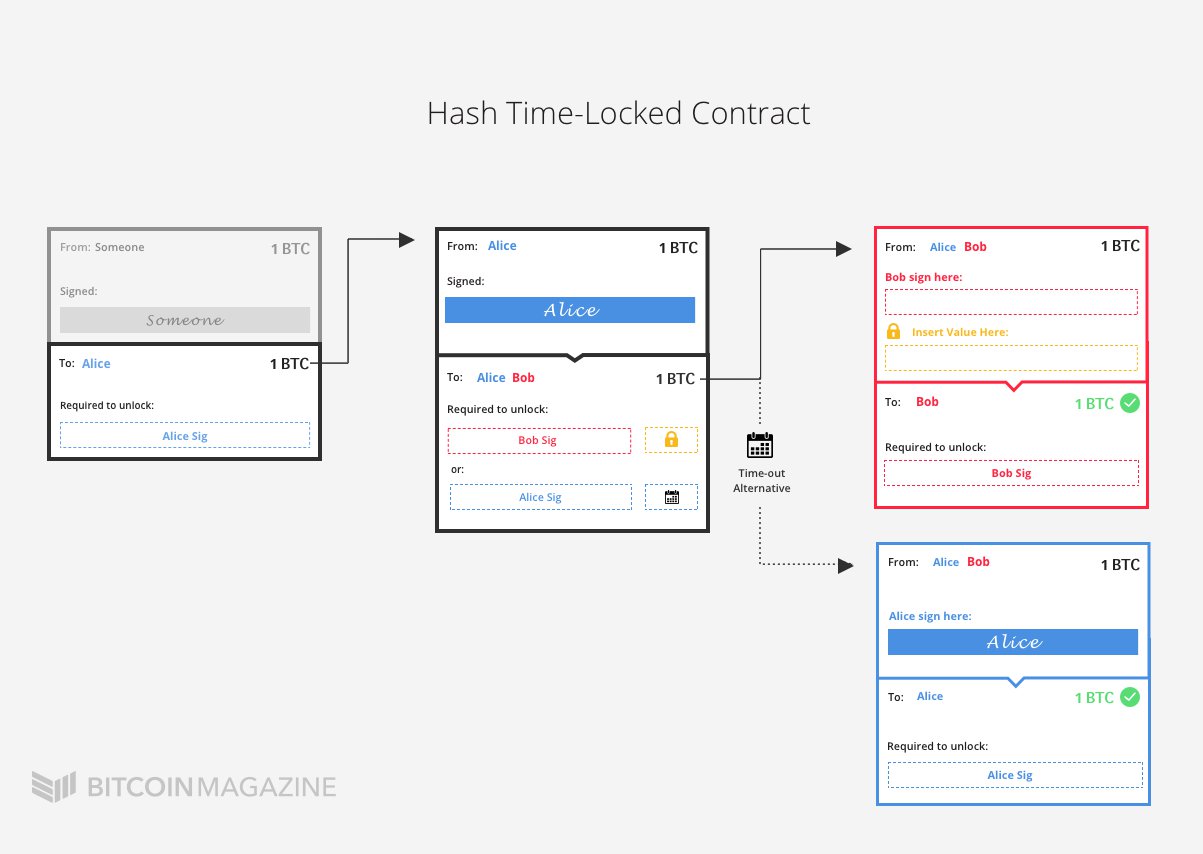
为了做到这一点，Alice没有直接给Bob发送一个比特币，而是把一个比特币发送到一个新的多签地址。锁定在这个地址上的比特币可以通过两种不同的方式解锁。

第一种选择是让Bob包含他的签名和密语。

第二种选择是让Alice自己签名。然而，还有一个CLTV时间锁：Alice只能在一段时间后进行签名和广播交易。

这意味着Bob有一段时间来创建一个后续交易，其中包括他的签名和密语，并通过广播将比特币从新的多签地址发送给自己。因此，这种交易是可靠的。Bob只能在提供密语的情况下花费Alice的比特币：通过比特币网络广播包含密语的交易。

如果Bob没有及时提供密语，那么Alice有一个“超时选择”可以取回她的比特币。

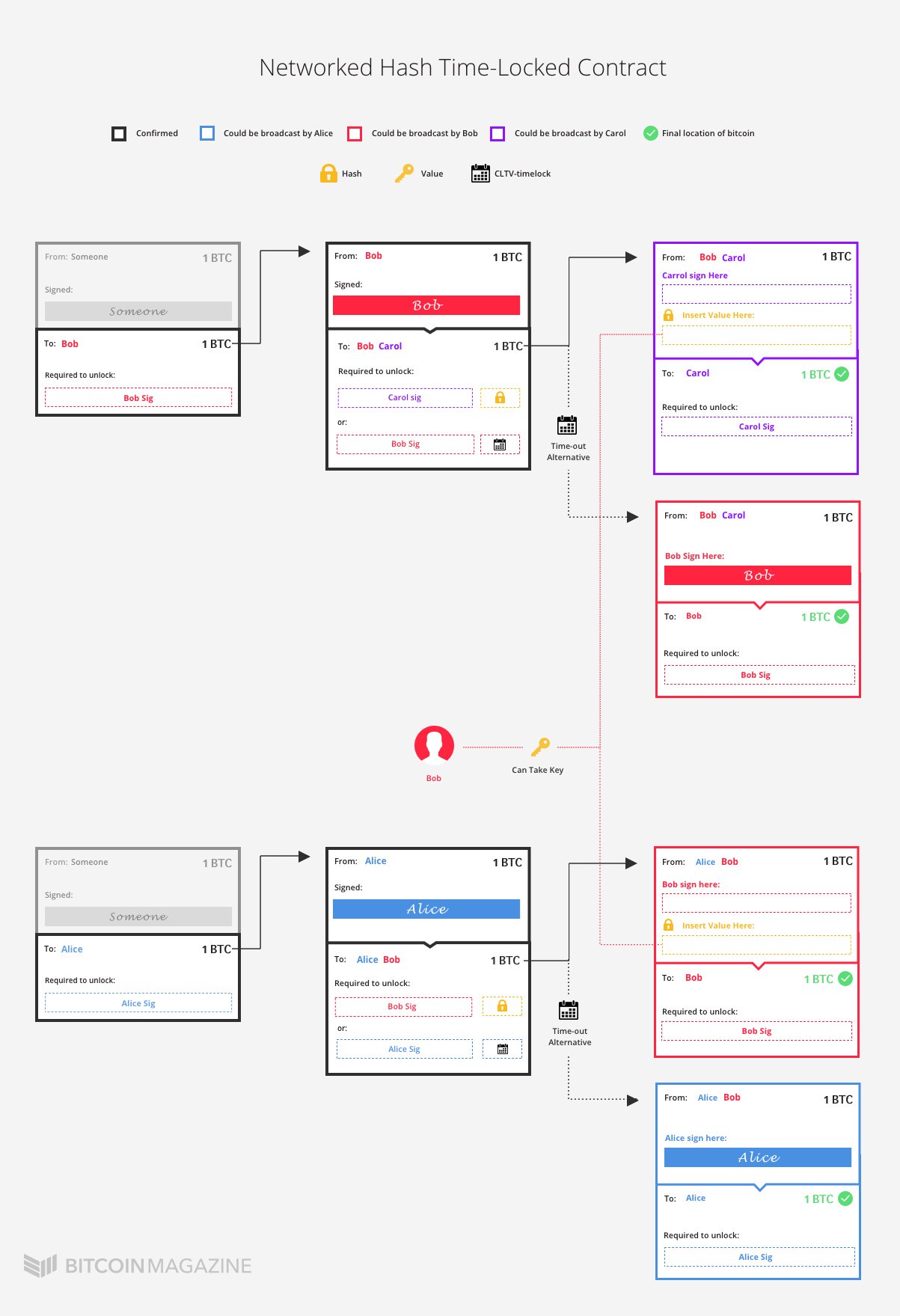


以上解释了为什么需要这个HTLC的原因。

如前所述，不仅Alice和Bob，还有Bob和Carol也建立了HTLC的交易。因此，如果Carol从Bob那里索要她的比特币，Bob将得到密语；它在区块链上是可见的。

因此，如果发生这种情况，Bob也可以从Alice那里得到比特币。Bob可以利用Carol在区块链上公开的密语，自己去花费Alice发送给他的比特币。这两个通道就连接起来了。

最后一个细节是，在Alice从Bob那里取回比特币之前，Bob需要从Carol那里得到密，这很重要。如果Bob在Alice收回她的钱后才从Carol那里得到密语，那么Bob终究还是被困在中间，他没有得到任何比特币。因此，Bob和Carol的HTLC的超时必须在Alice和Bob的HTLC的超时到期之前到期。



最后，还有一个问题需要解决：要使闪电网络真正可用，所有这些操作都必须在链下完成。如何做到这一点，将在本系列的第三篇也是最后一篇文章中介绍。