第一部分：构建比特币双向支付通道

闪电网络可能是部署在比特币之上最受期待的技术创新。2015年Joseph Poon和Tadge Dryja首次提出支付网络，在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、Blockstream和Blockchain——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。

在这里有三个部分组成的系列，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。

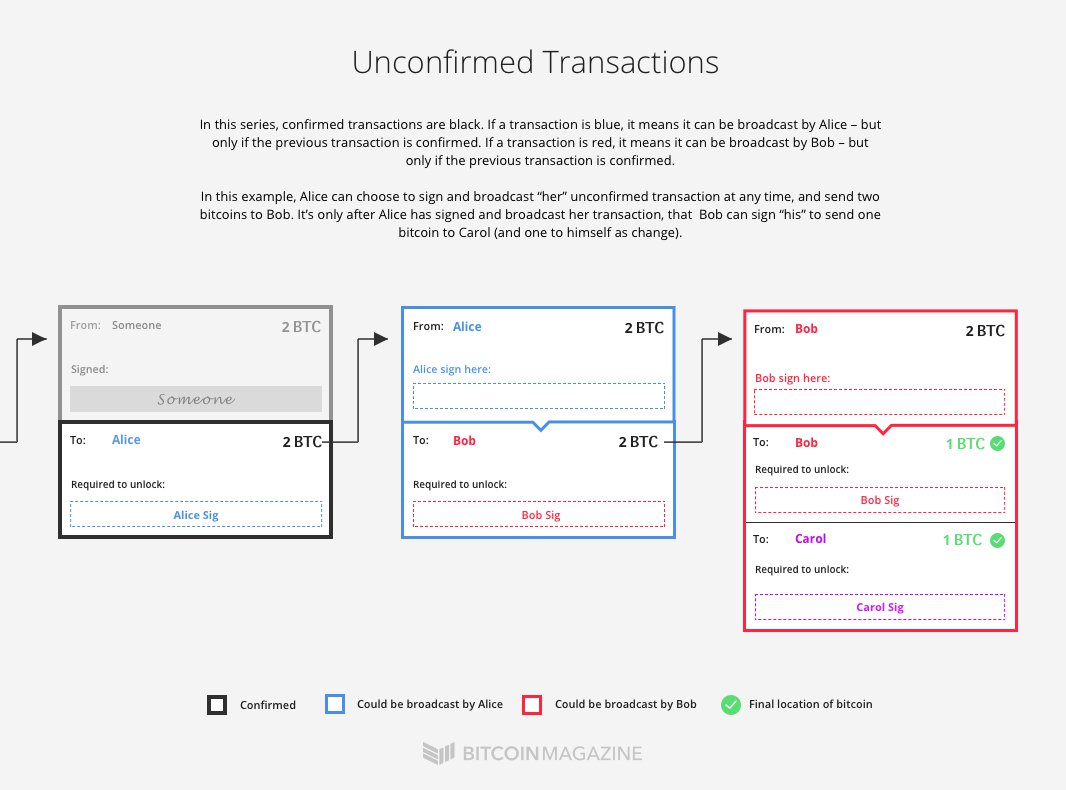
本系列的第一部分描述了必要的组成部分，并展示了如何将这些组成部分组合起来创建“智能合约”，应用于实现闪电网络的第一个要求：双向支付通道。

（注：任何对比特币有深入了解的人都可以跳过基本组成部分。）

组成部分1：未确认的交易

比特币协议的核心是交易，这些交易通常与以前的交易相关联，并且可能与未来的交易相关联。每个交易都包含引用比特币发送地址的输入，以及引用比特币发送地址的输出。此外，输入必须包括发送比特币的要求，如证明输入地址“所有权”的签名。同时，输出建立新的需求，这些需求必须包含在后续交易的输入中。

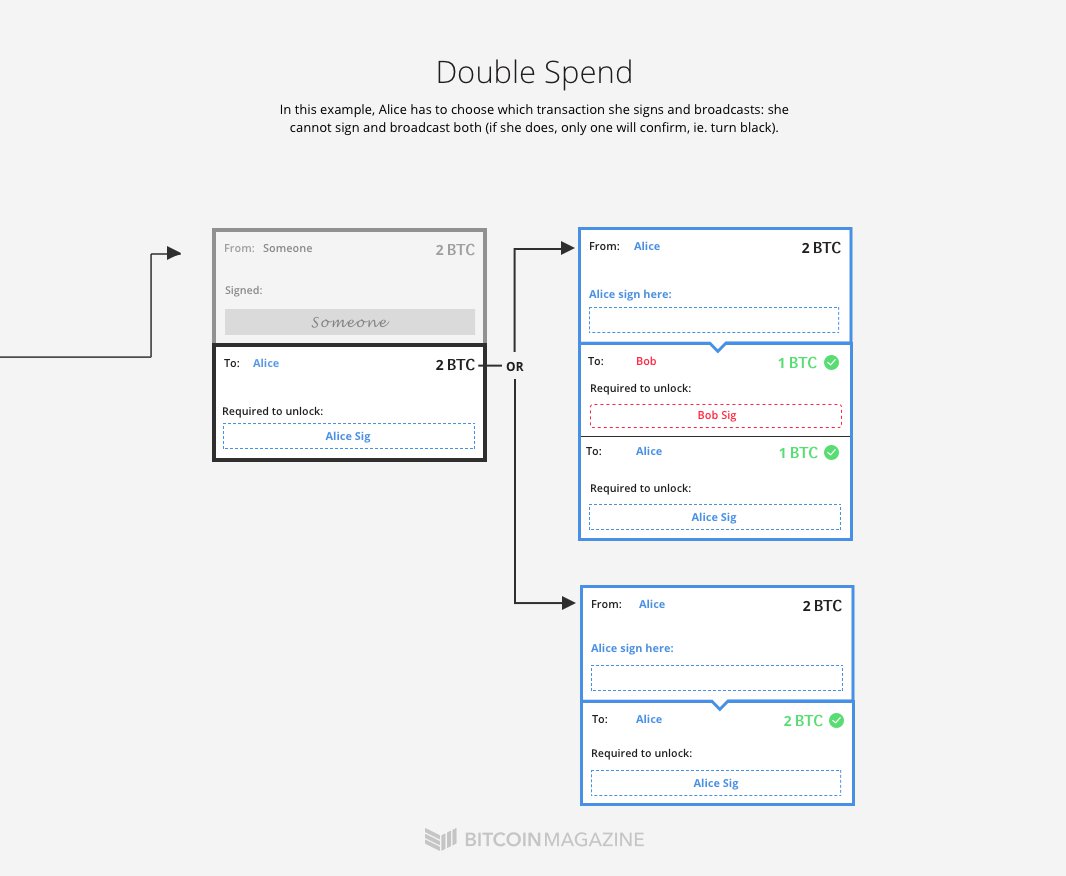
作为其主要功能之一，闪电网络是建立在或多或少的常规比特币交易之上。只是这些交易通常不会通过比特币网络进行广播。相反，它们存储在本地的用户节点上——但是它们可以在任何时候通过网络广播给比特币网络。



组成部分2：防止双花

闪电网络的第二个组成部分可能不需要太多的解释，因为比特币本身的就要求防止双花。如果两个交易（或：输入）依赖于相同的输出，则只有一个交易可以被确认。

这里要记住的重要一点是，未确认的交易可以发生双花，但只有一个交易可以被确认。

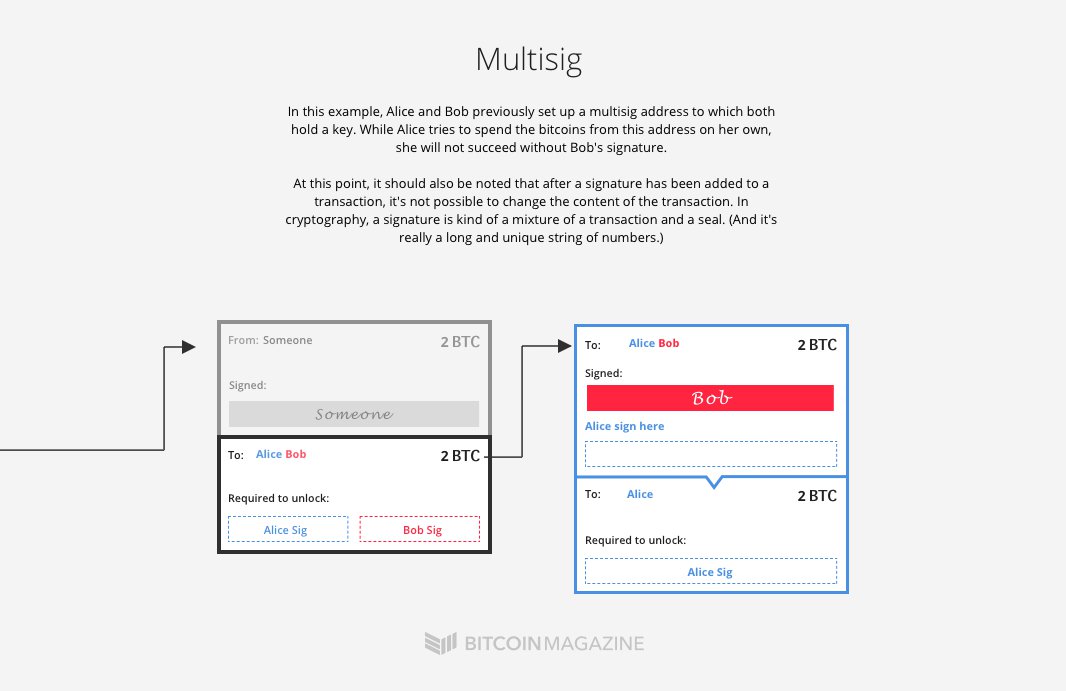


组成部分3：多签

闪电网络的第三个组成部分也很简单：多签（multisignature，multisig）地址。（或者更一般地说：p2sh地址。）

多签地址是比特币的一个地址，顾名思义，需要多个私钥才能“解锁”和使用比特币。多签地址可以根据需求来设置条件。例如，需要三把钥匙中的两把，或者十五把钥匙中的十五把，或者任何其他组合才能使用多签地址比特币。

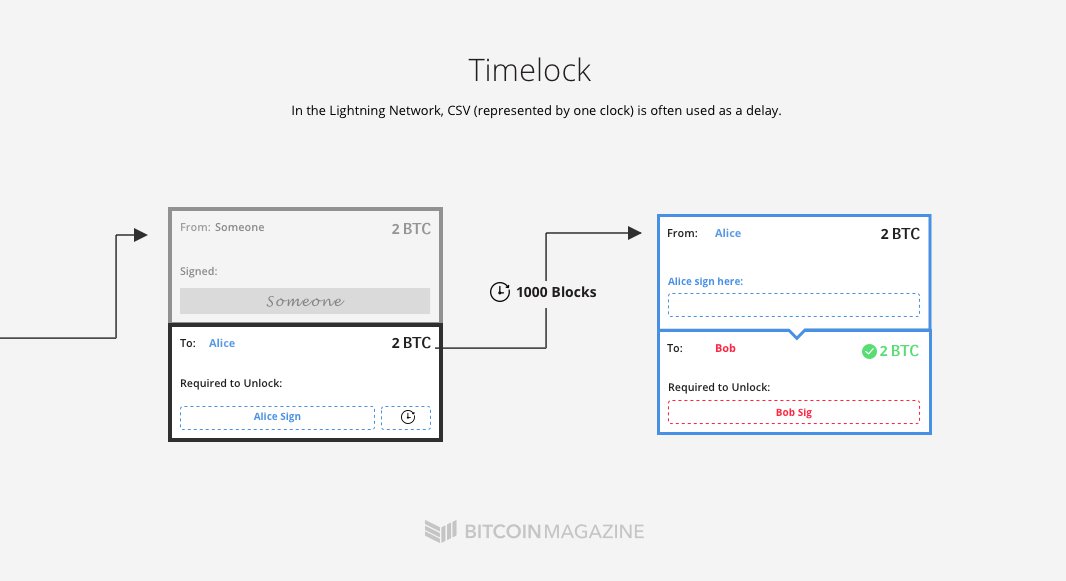
闪电网络通常使用2-of-2多签地址，从2-of-2的多签地址解锁比特币需要两个签名，这两个签名分别来自两个密钥。



组成部分4：时间锁

第四个组成部分是时间锁。时间锁可以在输出中“锁定比特币”，使其仅在未来某个时间点可消费（包括在后续输入中）。

有两种不同类型的时间锁：绝对类型，称为checklocktimeverify（cltv），相对类型，checksequenceverify（csv）。CLTV将比特币锁定到未来的（或多或少）具体时间：实际时间和日期，或特定的块高度。相反，csv使用相对时间。一旦一个cvs输出被记录在区块链上，在该比特币再次被使用之前，需要已经有从该点开始一个特定数量的区块。

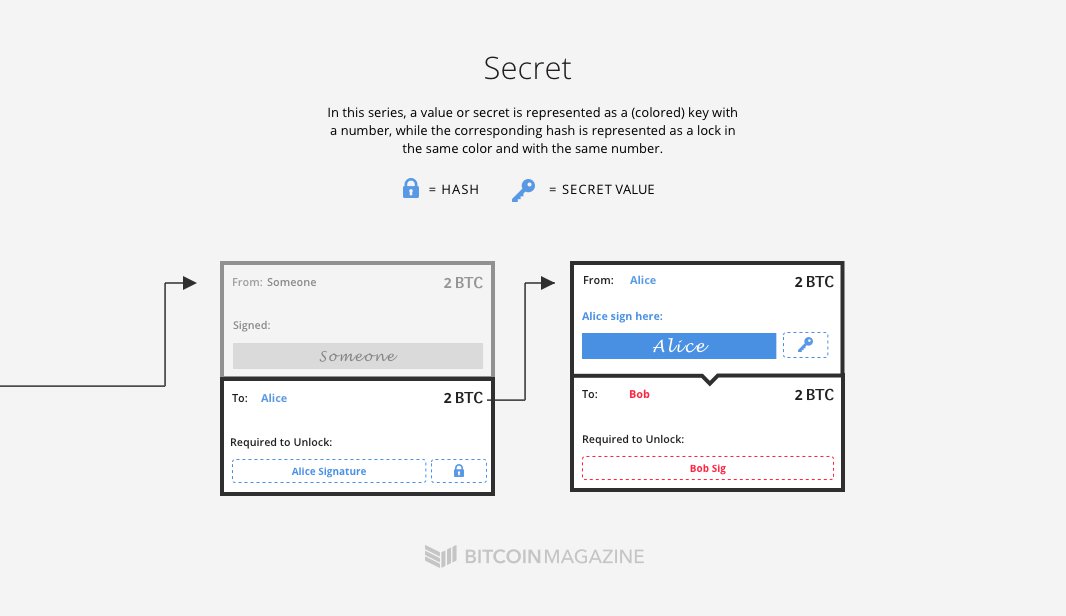


组成部分5：hash和密语

第五个也是最后一个组成部分——密语——是比特币本身最基本的组成部分。但在雷电网络中，它得到了新的应用。

简而言之，“值”或“密语”是一个很长且唯一的数字串，即使对于一台有无限次尝试的计算机，也几乎不可能猜到。通过特殊的计算，这个值（或密语）可以映射成另一个数字字符串，即hash。诀窍是：任何知道该值的人都可以轻松地复制hash。

这个技巧可以在比特币本身中使用，同样可以“锁定比特币”（事实上，比特币就是这样工作的）例如，hash可以包含在输出中，并且需要随后的输入包含相应的值，以便可以消费。



第一个挑战：双向支付通道

在闪电网络出现之前，支付通道的概念已经存在了一段时间。典型的支付通道在某些场景下是有用的，但也有局限性：它们是单向的。Alice可以向Bob支付几个链下交易，但Bob根本无法通过同一通道向Alice支付。

双向支付通道是闪电网络的一个重要特征，是Poon和Dryja提出的一种无信任的双向支付通道。

打开通道

要建立双向支付通道，双方必须首先就交易达成一致，这决定了双方存入通道的比特币数量。

假设Alice想给Bob发送一个比特币。由于Alice和Bob之间的交易可能会很频繁，他们决定开通双向支付通道，并以此发送比特币。

为了打开这个支付通道，Alice和Bob每个人都会将5个比特币发送到一个2-of-2的多签地址。这是“期初交易”，只有Alice和Bob在随后的交易上签名，比特币才能从这个地址被花费。

另外，Alice和Bob都创建了一个密语（一串数字），并交换密语hash。

Alice现在立即从期初交易创建一个后续交易。这是一个“承诺交易”。在承诺交易中，Alice给自己发送了四个比特币，给第二个多签地址发送了六个比特币。第二个多签地址有点奇怪，它可以由Bob自己解锁，但只有在区块链中包含了1000个额外的区块之后才能解锁；同时它包含一个csv锁，Alice可以自己打开它，但前提是她有Bob刚刚给出的密语。（当然，Alice不知道这个密语是什么——她只知道密语的hash——所以她现在无法使用这个交易输出。）

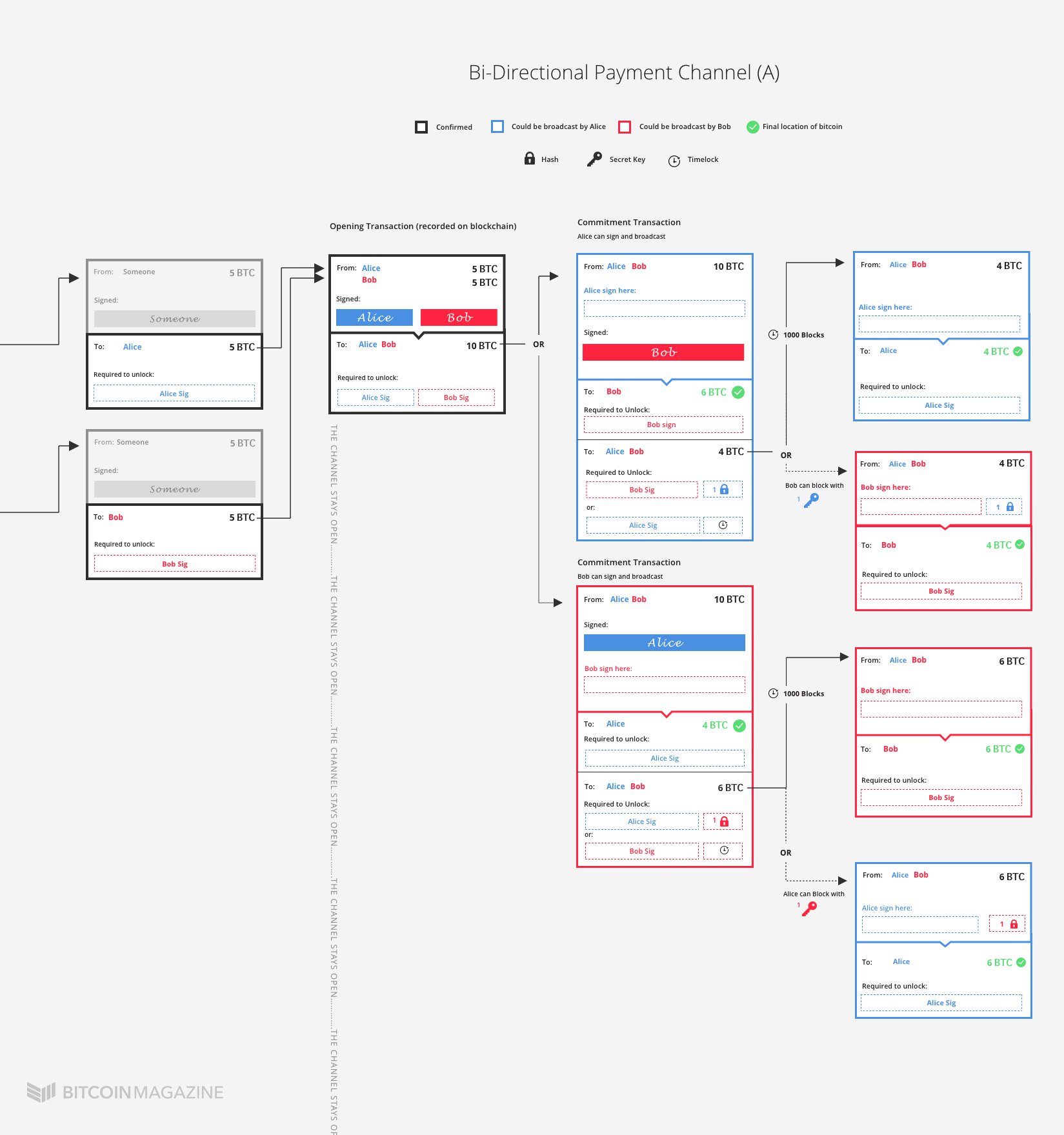
Alice在这项承诺交易上签名。但她没有广播！相反，她把它给了Bob。

同时，Bob也做了同样的事。他创建了一个承诺交易，在承诺交易中，发送6个比特币给自己，发送4个比特币到一个多签地址。如果Alice再等1000个区块，她可以解锁这个地址，或者Bob可以用Alice的密语解锁。

Bob在这项承诺交易上签名，发送给了Alice。

在所有这些“半有效”承诺交易和密语的hash交换之后，他们都签名然后广播了期初交易，以确保它被记录在比特币区块链上。该通道现在正式打开。

此时，Alice和Bob都可以签名并广播从另一方获得的半有效承诺交易。如果Alice这么做了，Bob马上就得到6个比特币。如果Bob这么做，Alice马上就得到4个比特币。但是，任何人签名和广播交易将不得不等待1000区块之后才能解锁多签地址中的比特币，才能使用剩余的比特币。



然而，这里一个支付通道的关键点：既不签名也不广播他们的半有效交易。

更新通道

过了一会儿，Bob想给Alice发送1个比特币。他们想更新通道状态，使余额再次达到5-5。为了做到这一点，Alice和Bob做了两件事。

首先，两者都重复上述过程（除了期初交易已经记录在区块链上）。这一次，Alice和Bob都将自己归为5个比特币，并且都将5个比特币归为多签地址。这些多签地址的条件设置是相似的，除了它们需要新的密语：Alice和Bob都提供彼此新的密语哈希。他们都签名了新的半有效承诺交易，并将其交给对方。

第二，Alice和Bob交换了他们各自在第一次中使用的密语。

在这一点上，Alice和Bob可以再次签名和广播他们刚刚得到的新的“半有效”承诺交易。他们的对手将立即获得5比特币，而广播交易的自己将不得不等待1000个区块。这样通道完成更新。

但是，是什么阻止了Bob广播旧的承诺交易呢？旧的承诺交易可以导致支付给他6比特币而不是5比特币。

阻止Bob的当然是他的第一个密语，现在他已经把这个密语告诉了Alice。

Bob不能再安全地签名和广播旧的承诺交易，因为Alice现在知道Bob的第一个密语。如果Bob签名并广播旧的承诺交易，他会立即将4比特币发送给Alice……他要等1000个区块才能拿到自己的6比特币。然而，因为现在Alice知道了他的密语，她可以利用这段时间来击败Bob，并可以获得另外的6个比特币！

既然Bob也有Alice的密语，反过来也一样。如果Alice试图签名和广播一个旧的承诺交易，Bob可以获得通道上的所有比特币。

当然，这意味着Alice和Bob都被强烈地激励着去公平竞争，而且仅仅签名和广播通道的最新状态。

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。2015年Joseph Poon和Tadge Dryja首次提出支付网络，在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真的会给他密语，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）

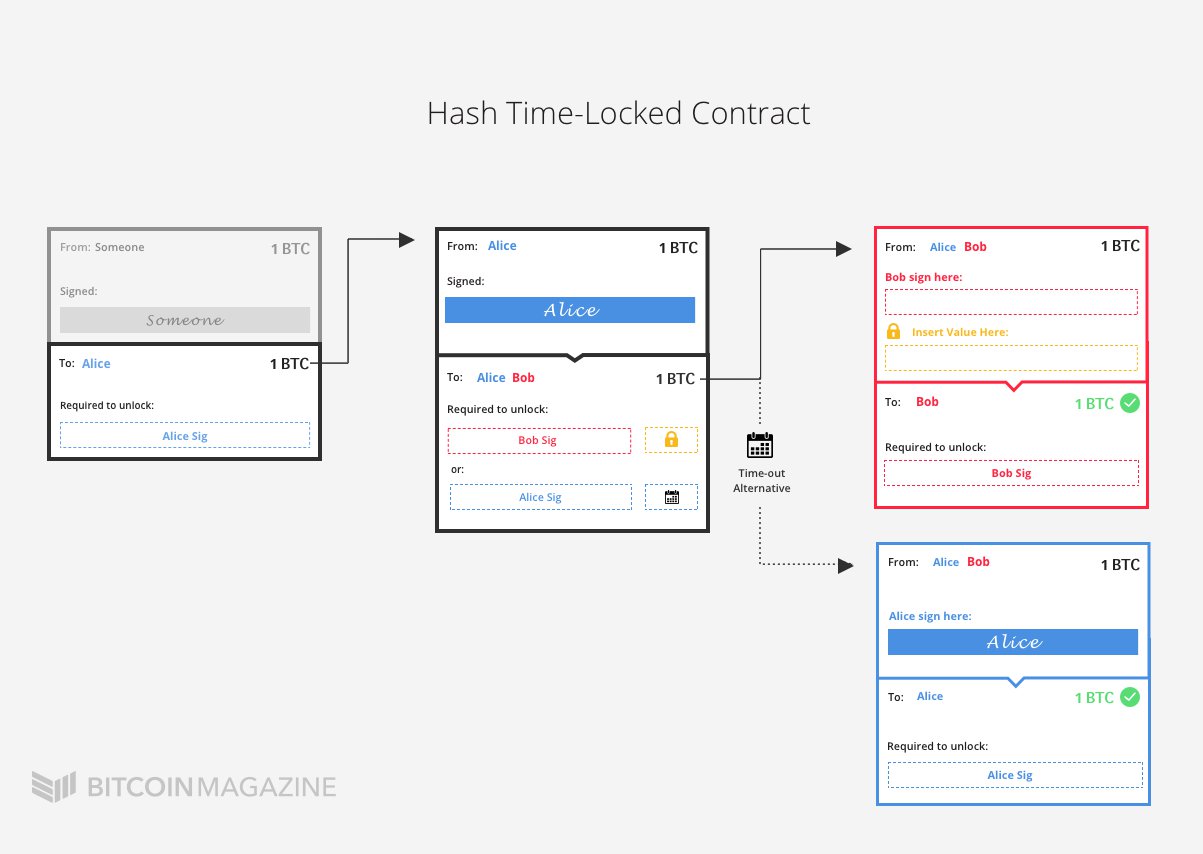
为了做到这一点，Alice没有直接给Bob发送一个比特币，而是把一个比特币发送到一个新的多签地址。锁定在这个地址上的比特币可以通过两种不同的方式解锁。

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。

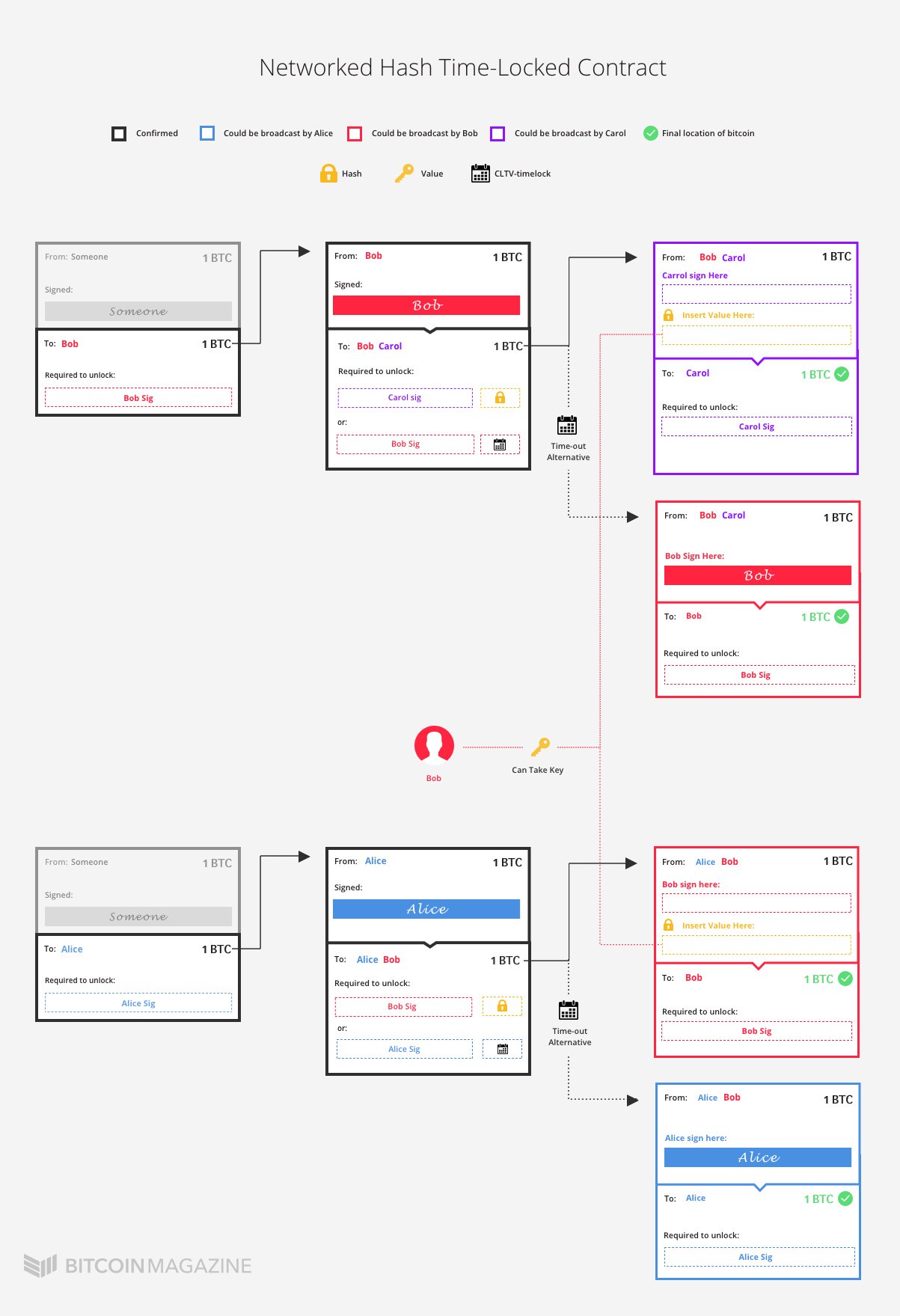


以上解释了为什么需要这个HTLC的原因。

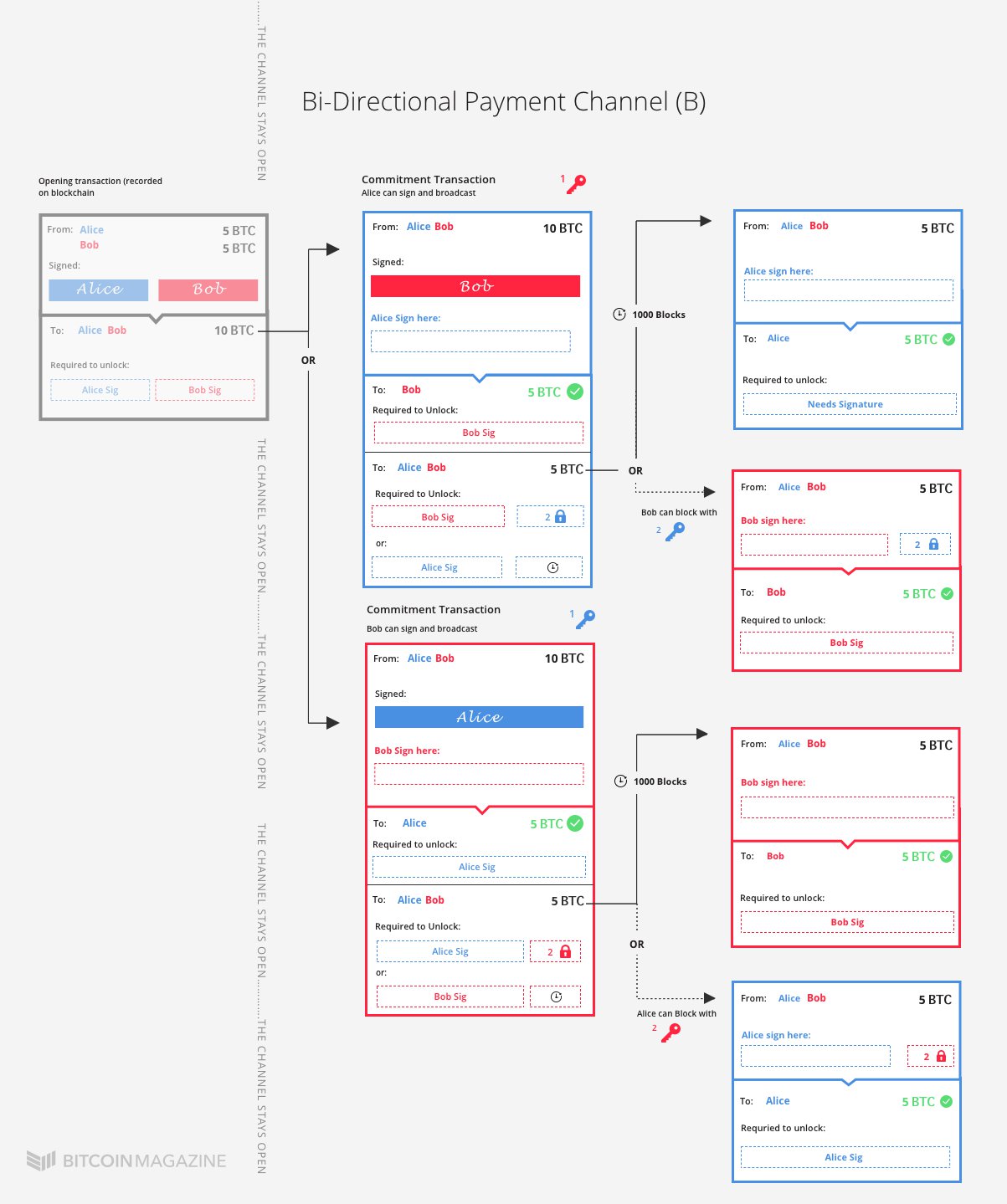
如前所述，不仅Alice和Bob，还有Bob和Carol也建立了HTLC的交易。因此，如果Carol从Bob那里索要她的比特币，Bob将得到密语；它在区块链上是可见的。

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。



这个双向支付通道需要扩展以允许通过网络进行支付。这将在本系列接下来的第二篇文章中介绍。