### 了解闪电网络，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。约一年前（2015）由Joseph Poon和Tadge Dryja首次提出的支付网络，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。

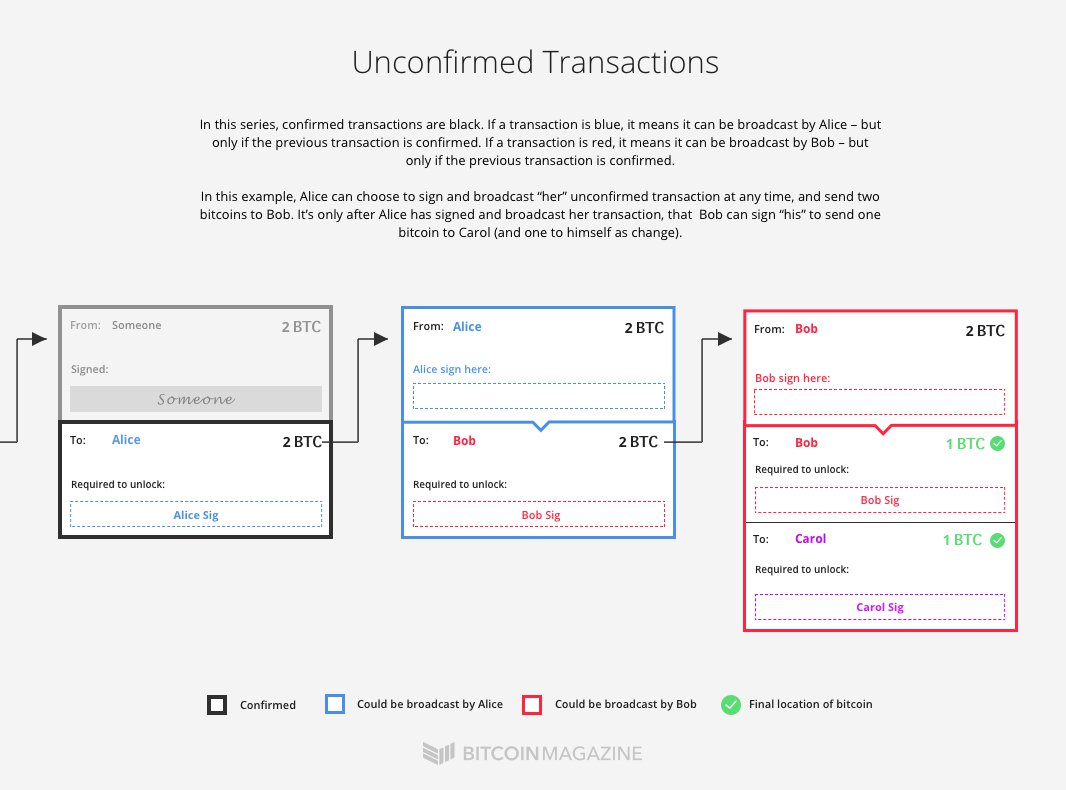
本系列的第一部分描述了必要的组成部分，并展示了如何将这些组成部分组合起来创建“智能合约”，应用于实现闪电网络的第一个要求：双向支付通道。

（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事务的输入中。

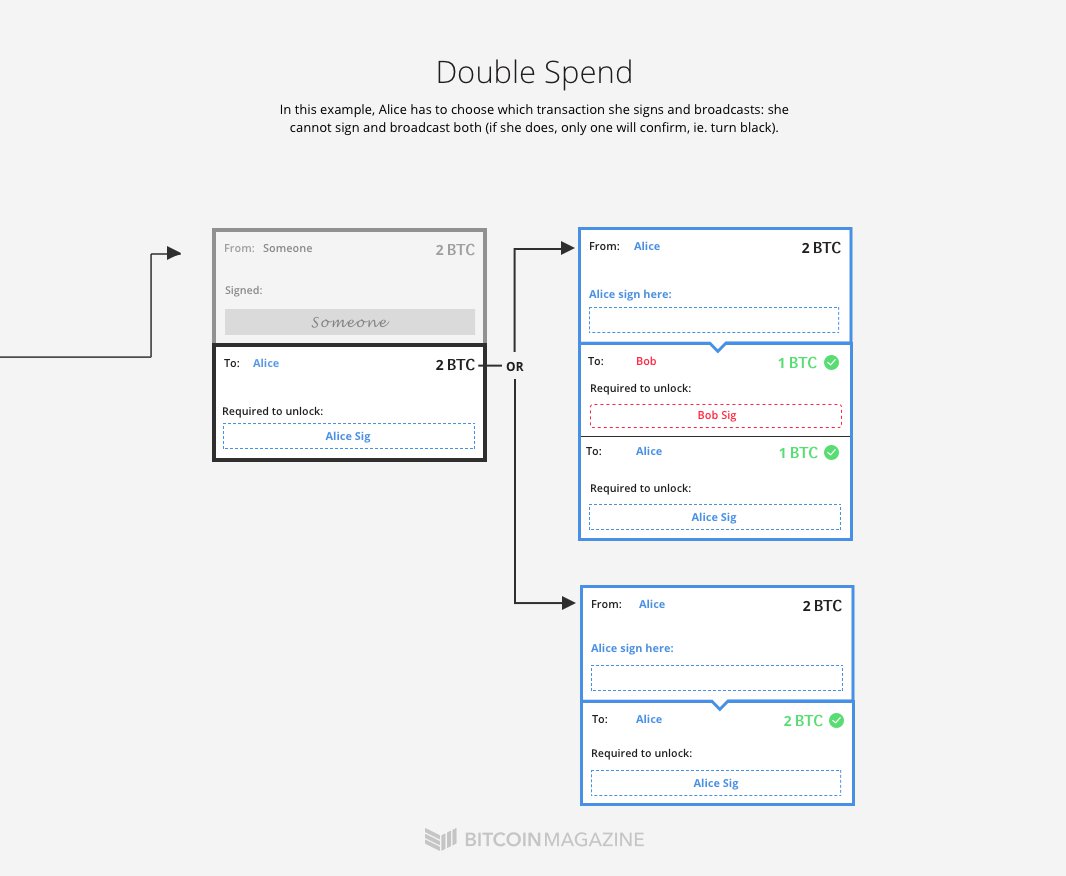
作为其主要功能之一，闪电网络是建立在或多或少的常规比特币交易之上。只是这些交易通常不会通过比特币网络进行广播。相反，它们存储在本地的用户节点上——但是它们可以在任何时候通过网络广播给比特币网络。



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。

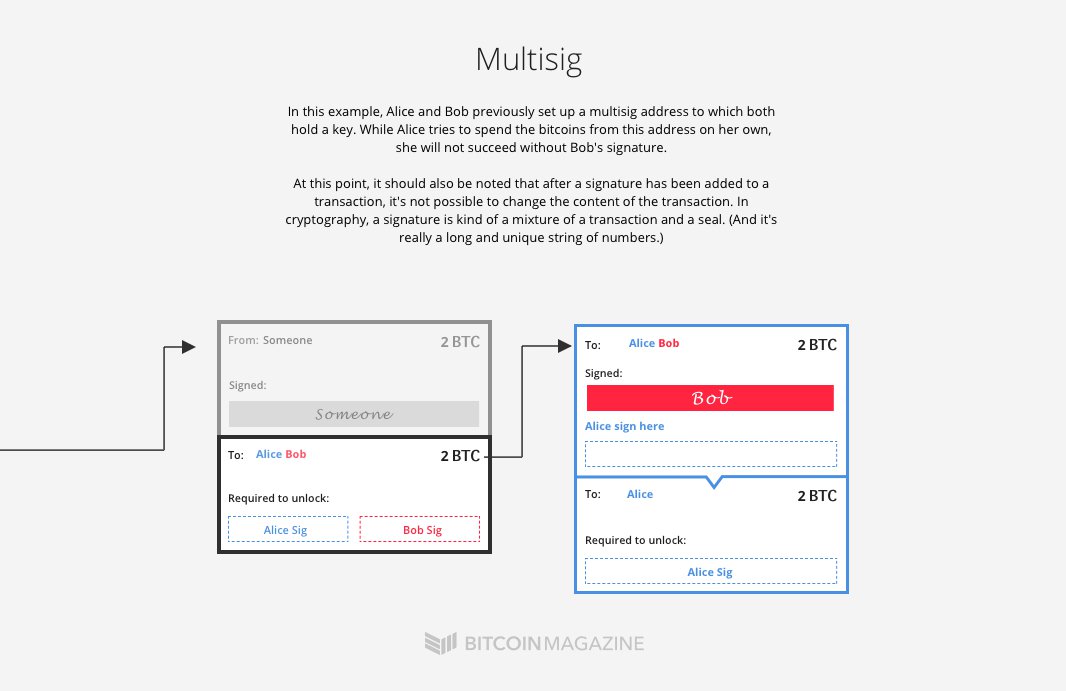


组成部分3：多签

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。

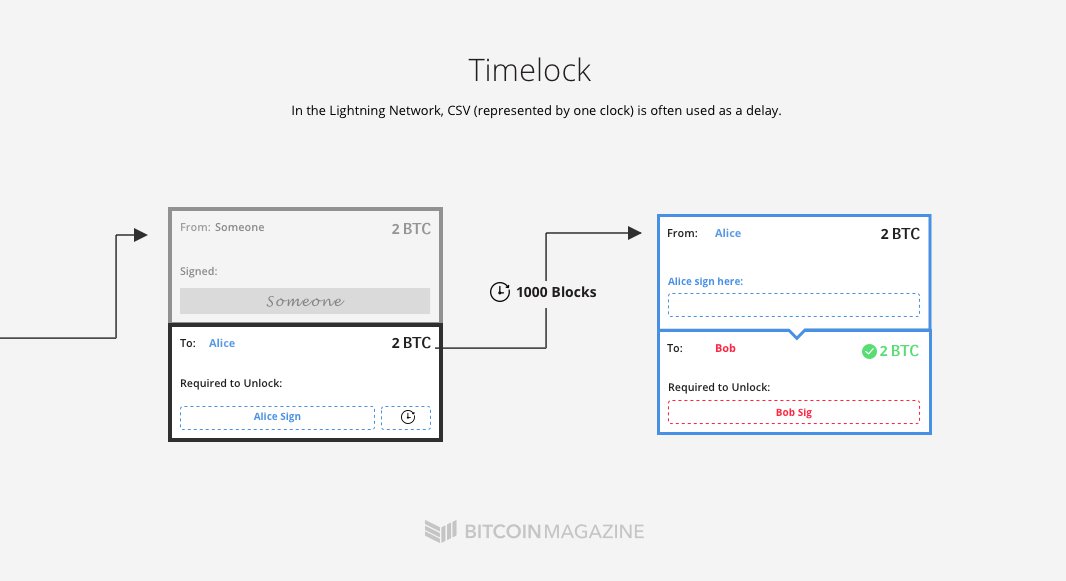
闪电网络通常使用2-of-2多签地址，从2-of-2的多签地址解锁比特币需要两个签名，这两个签名分别来自两个密钥。



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。

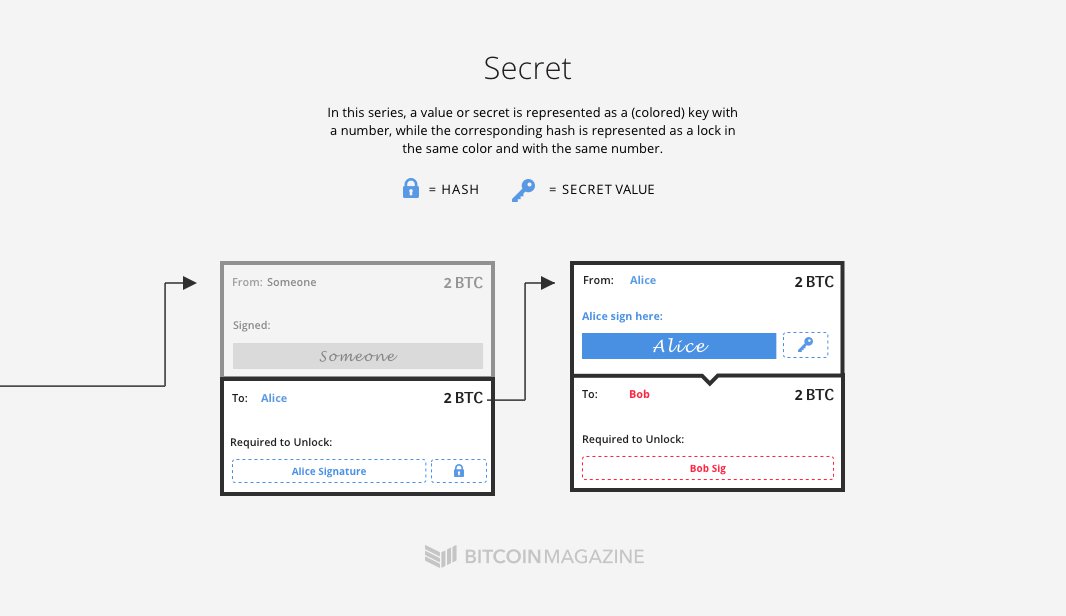


组成部分5：hash和密语

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。）

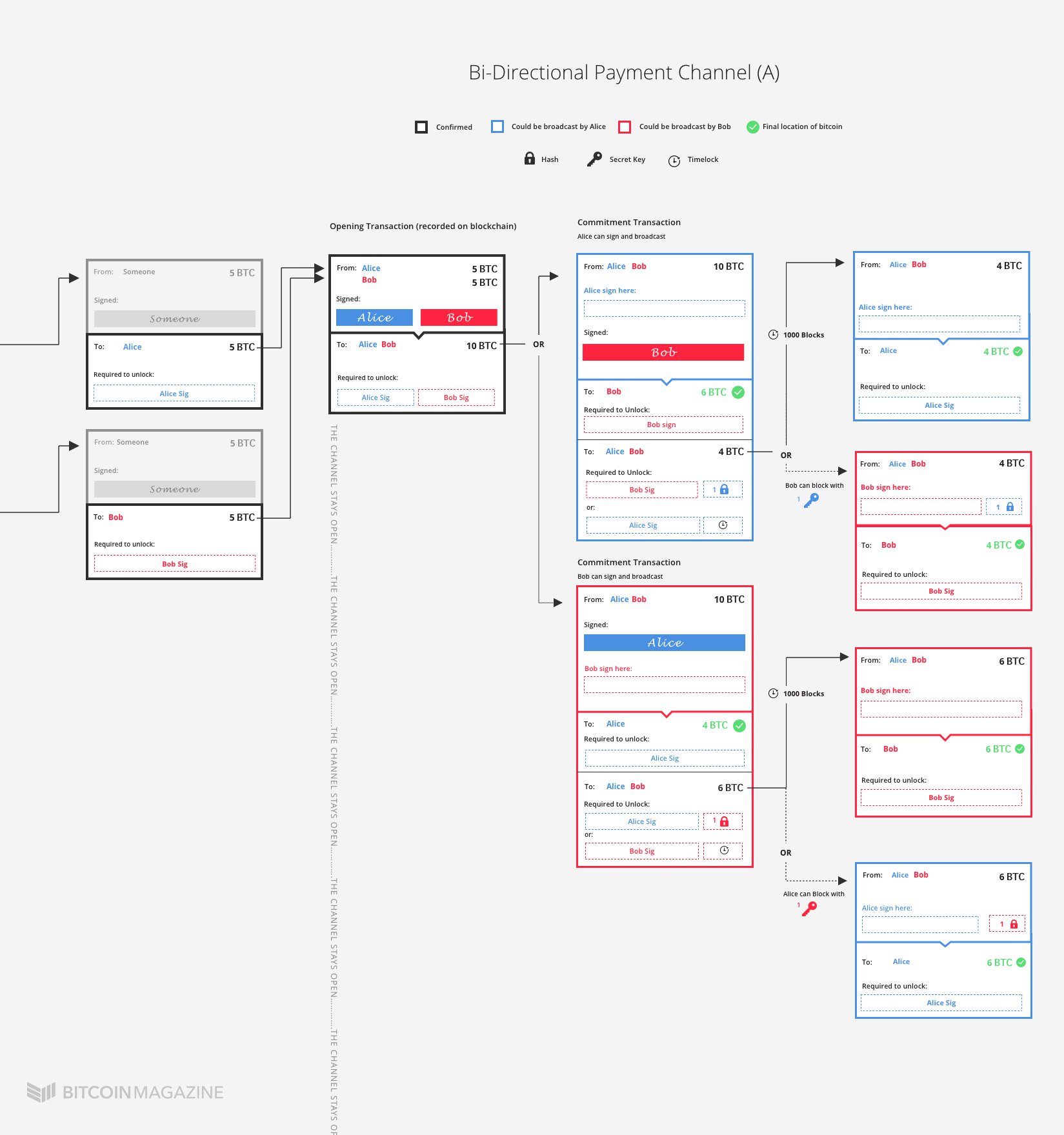
Alice在这项承诺交易上签名。但她没有广播！相反，她把它给了Bob。

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。

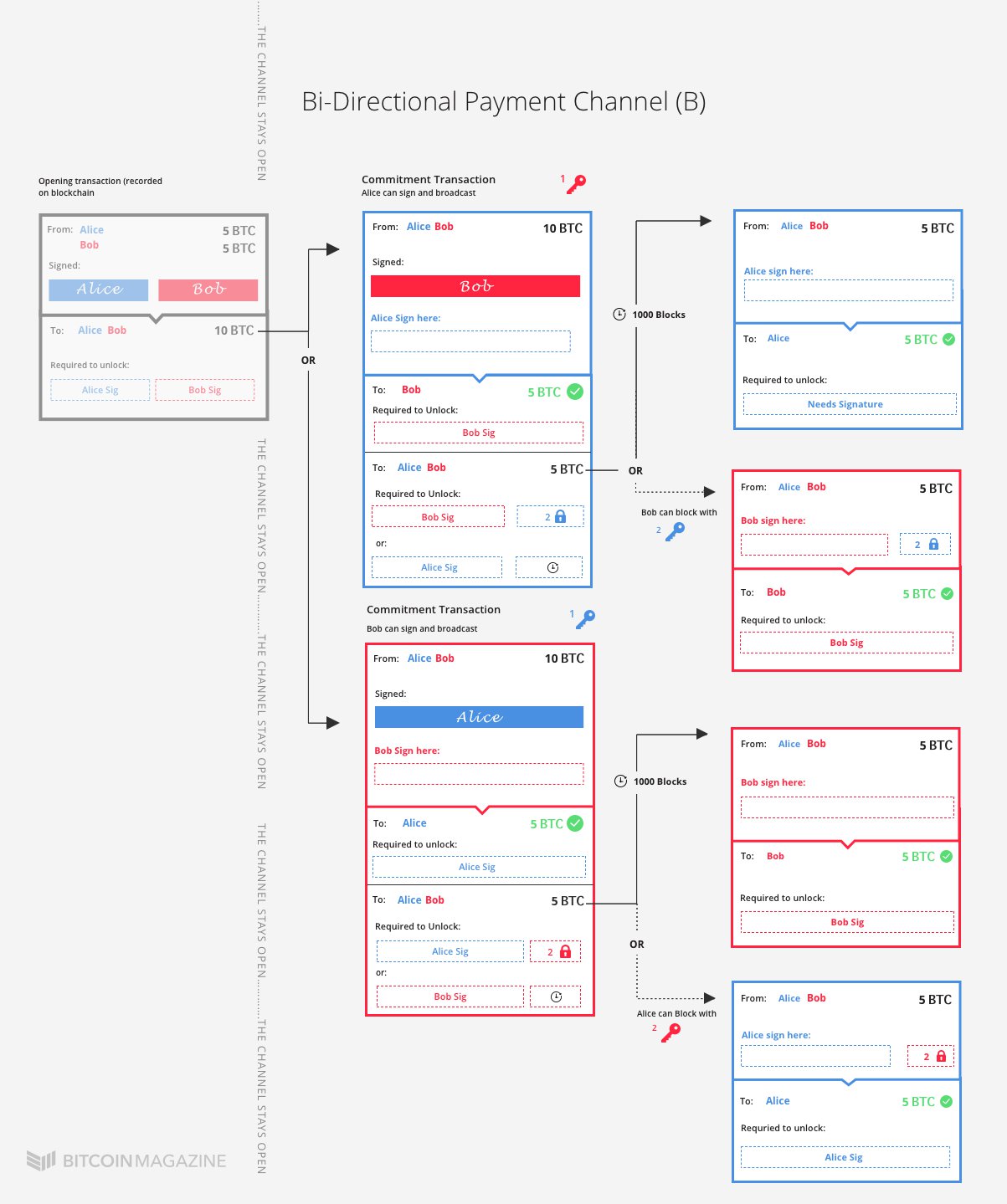
但是，是什么阻止了Bob广播旧的承诺交易呢？旧的承诺交易可以导致支付给他6比特币而不是5比特币。

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。



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。

路由和关闭通道

闪电网络可能是部署在比特币之上最受期待的技术创新。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。）

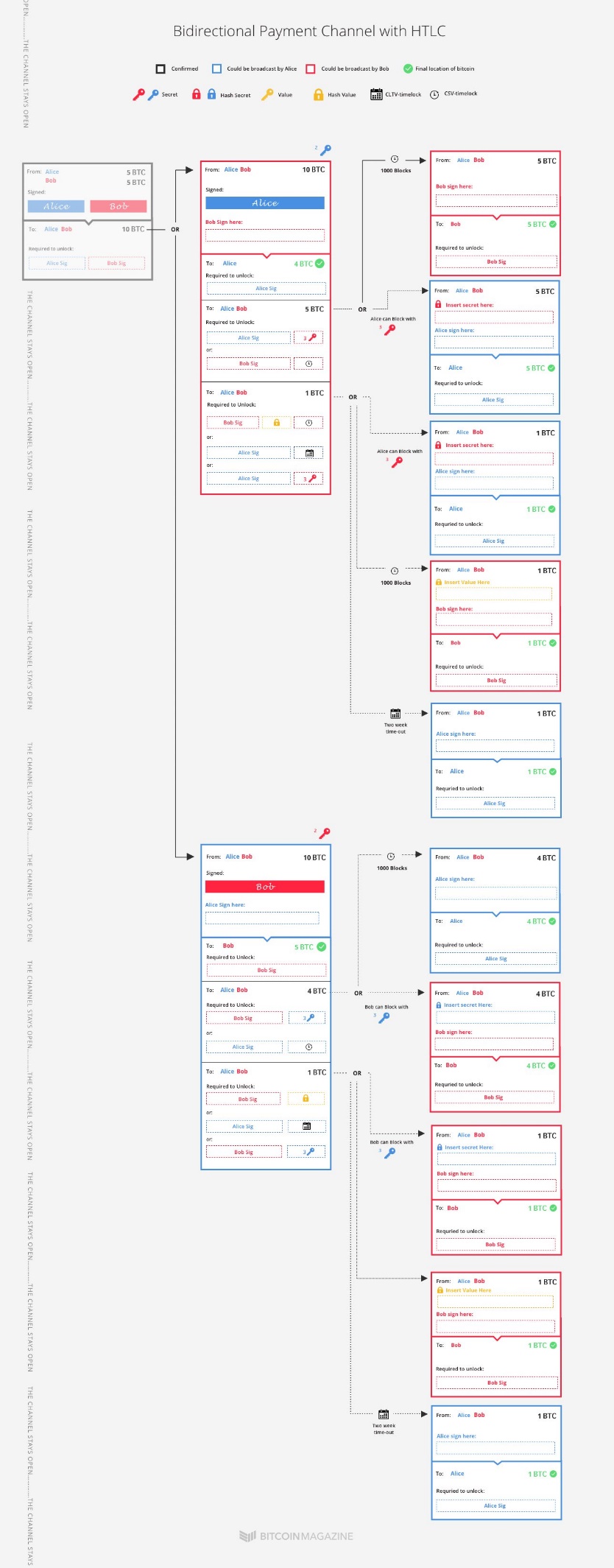
第三，与任何其他HTLC一样，这两项承诺交易也包括Alice通常的CLTV超时。如果Bob没有在一段时间内提供密语，比方说——两周内（例如，因为他没有从Carol那里得到），Alice就可以收回她的比特币。

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。



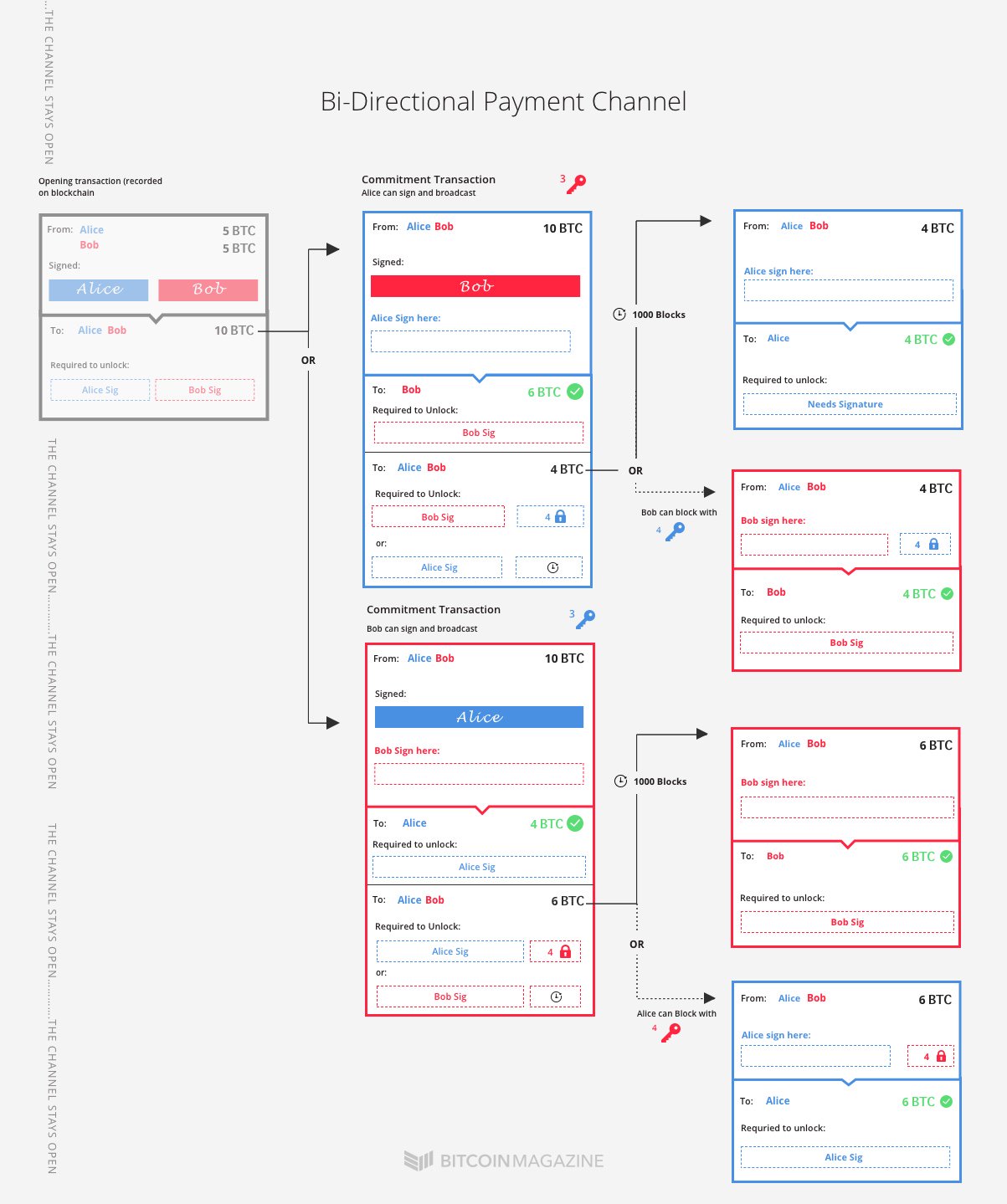
安装状态通道

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。

