闪电网络怀疑论

[**王二**](http://www.8btc.com/author/8843)**2015-12-29 07:30 发布在**[**区块链**](http://www.8btc.com/blockchain)[**2**](http://www.8btc.com/skepticism#comment)**2843**



我喜欢闪电网络这个点子。在我看来，闪电网络背后的开发者们很聪明，而且选择利用比特币协议这一点也是非常精明的。我相信闪电网络中的任何一项东西都是有利于比特币生态圈的。然而我不赞成的是，闪电网络能否顺利替代比特币还是个未知数，现在就开始过早地贬低比特币核心（零配置网络交易和低交易费）。然而，这似乎就是那些核心开发人员一心想要做的事。

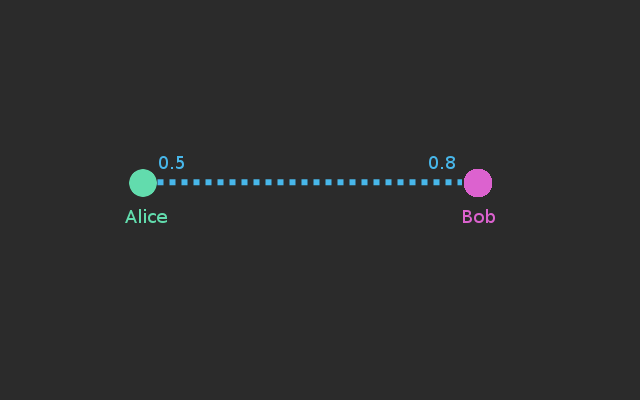
我们知道，至少闪电网络在技术上是具有可行性的。我们只是不知道它是否为一个兼具经济可行性，甚至说是一个称心如意的替代方案。它是会变成分散的对等支付层？还是说最终仍像现代银行一样的准集中式的支付网络？我们都不得而知，除非我们将其付诸于实践，而这也正好说明全部押在闪电上不负责任的。

起初我主要担心的是，作为一个中转站辐射型支付层，它只有很少的中转站，准集中型网络和一个易受攻击的调节器。而且似乎不只有我一个人存在这样的疑虑，由于最新支点的出现并不同于其他中心辐射型网络拓扑结构，它变成了一种更有组织的、钱包对钱包的路径。这种网络结构可以设想为没有那些大型支付层的，更加纯净的p2p支付层。

当然，因为它已经印证了我最初的疑虑，所以这个发展情况还算在我意料之中。但不幸的是，我觉得闪电网络的这个观点太过乐观了。接下来我会给出闪电网络的一个概况，并阐述一些理由来说明我为什么会认为这种网络结构很有可能以中心辐射型拓扑结构（hub-and-spoke topology ）形式结束。

闪电网络的工作原理

闪电网络的核心概念，也就是支付渠道。使用一些复杂的比特币脚本，双方就可以建立一个“渠道”，这个“渠道”一旦被打开，就可以让他们做成无数笔无需信任的“链下”交易。

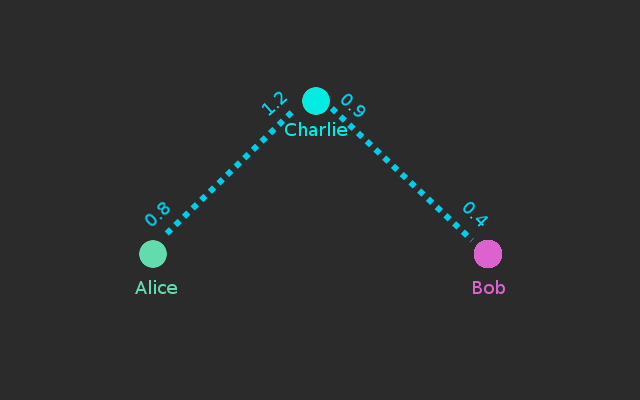


为了打开这个渠道，双方需要共同建立一笔交易，交易中的一方或者双方需要将比特币存入这个渠道中，然后这笔交易再被转移到比特币区块链中。在上图所示的例子中，爱丽丝在渠道中投入了0.5比特币，而鲍勃在渠道中投入了0.8比特币。

当要关闭这个渠道时，双方中的任意一方均有一秒的反应时间，比特币网络的链上交易将替双方支付这次交易所需费用。然而，当这个渠道处于开放状态时，双方在任何时候都可以不通过上链交易就可以共同协商修改支付分配。比如说，当爱丽丝想要支付鲍勃0.1BTC时，他们可以更新支付分配，其中鲍勃可以得到0.9BTC，爱丽丝则会得到0.4BTC。而只要这个通道一直处于开放状态，那他们就可以无限制的进行交易。

渠道网络

考虑以下因素就可以看到这是如何扩展为一个支付网络的：

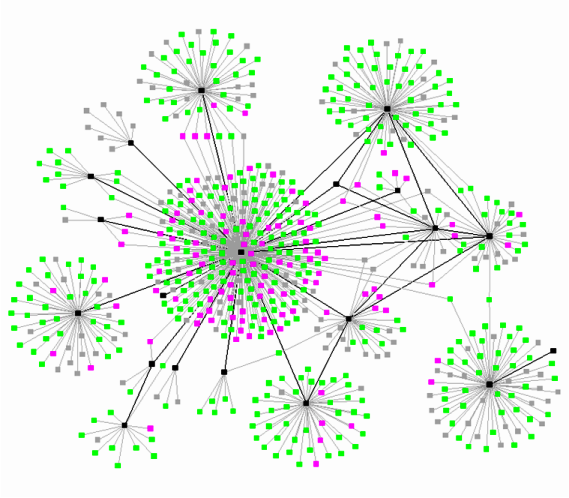


如上图所示，爱丽丝想要支付0.5BTC给鲍勃，但她并没有一个渠道来和他进行交易。幸运的是，她和查理有一个交易渠道，而查理正好和鲍勃有一个交易渠道。这样爱丽丝就能借助查理的交易渠道，通过 hashed timelock contract（HTLC）来和鲍勃进行交易了。

为了完成这次交易，爱丽丝就会给鲍勃发短信说：“嘿！我要给你付笔款。”这时鲍勃自己将收到一个随机数字(R)，接着鲍勃便会回一个被hash的数字（H）（你可以认为被hash的数字R是随机数字的一种加密形式）给爱丽丝。然后爱丽丝的钱包紧接着就会联系查理说：“嘿，查理。如果你给我生成（H）的未加密值(R)，那么我就同意更新我们渠道的支付分配，这样你就可以得到的就会比0.5BTC多一点，我得的比0.5少一点。”尽管查理并不知道R，但他也会同意。之后查理便会去找鲍勃说：“嘿，鲍勃。如果你给我那个能生成H的未加密的值R，我将同意更新我们渠道的支付分配，这样你就可以得到的会比0.5BTC多一点，我得到的比0.5少一点。”

因为R就是从鲍勃这里生成的，所以他肯定知道。接着他马上将R告诉查理，并更新了其渠道的支付分配。然后查理将R告诉给了爱丽丝之后也更新他们的渠道，最后交易完成，爱丽丝以脱链的形式付给鲍勃0.5BTC。

闪电网络的最初设想为一个中心辐射型网络。



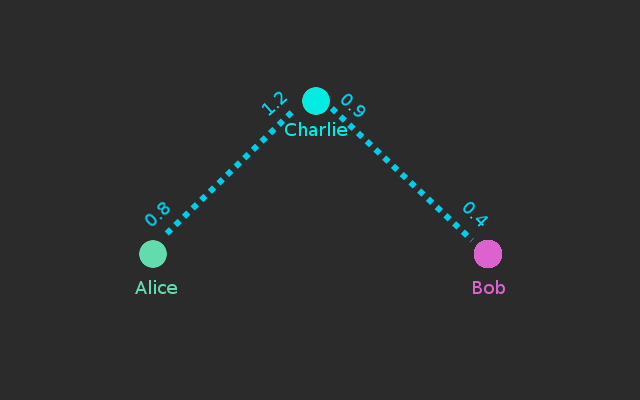
你的钱包将会连接到一个“支付中转站”，也就是上述例子中查理所扮演的角色。由于各种支付渠道彼此之间都保持畅通，爱丽丝有一个和中转站A相通的渠道，而鲍勃也有一个和中转站B相同的渠道，这样爱丽丝就可以直接和鲍勃交易了。和之前的比起来，用相同的办法现在只需要在彼此间有一到两个额外跳跃就可以完成。

如果能有许许多多的小额支付中心（成百或上千个），那么这个网络拓扑结构就能完美运行。但是，若是只有少数几个大型中转站，那么这个网络拓扑结构就会完全失败。它就是下一个visa卡、万事达卡或者美国运通。

那需要多少个中转站？

要精确地预测出存在于网络均衡中的中转站的数量是完全不可能的，但是仍有一些理由可以说明这个数字是会逐渐变小，而不是增加。然而不可否认的是，这是一款开源性的软件，任何人都可以在上面运行一个支付中转站(至少在政府部门决定监管之前)，只是支付中转站运行的高成本就像是给进入者们形成了一道坚固的壁垒，从而也就产生出了集中式压力。

我在讨论什么样的成本呢？让我们回到查理扮演“交易中转站”的那个例子中去。



回想一下，爱丽丝需要（通过查理）把比特币付给鲍勃，所以查理不得不在更新他和爱丽丝的分配渠道之前就更新他与鲍勃的分配渠道（付给鲍勃的多，自己得到的要少）。也就是说，查理在得到鲍勃的0.5BTC之前（一段很短的时间内），就得先付钱给爱丽丝。

这意味着，如果查理想要成为一个支付中转站，那他自己必须在他“客户”共有的渠道里存够足够多的比特币，这样才能促成这些“客户”的脱链交易。如果查理没有预存至少0.5BTC(今天换算过来应该是420$)到鲍勃的渠道里，那么这笔交易就不能做成。

现在，这笔钱不会以任何形式来构成贷款，查理将保留其百分之百的控制权。但是，这笔钱至少还是需要放在那些渠道里，以便促成那些脱链支付。我们知道，钱的时间价值是一个东西，所以要运行一个支付中转站还是需要一些切切实实的成本的。更不用说在你刚开始之前就需要拿出一大笔钱了。

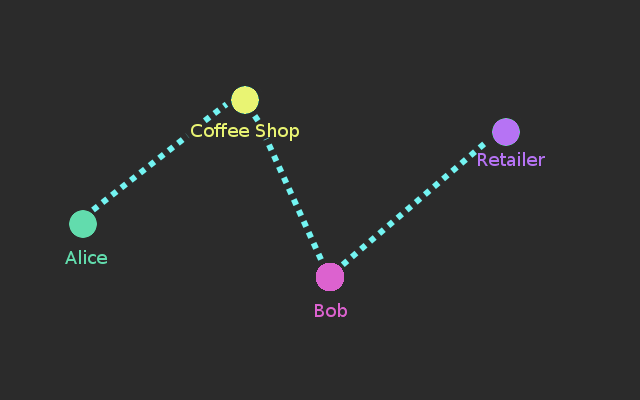
那一个支付中转站应该给每个渠道存入多少预存款呢？我并不知道，我们只能说这是价值500$的比特币。如果你想要运行一个服务100人的支付中转站，你需要50000$的资产来启动它（更现实一点的话，这个数字将会变为百万）。我碰到的一些媒体人似乎认为人们在卧室就可以运行他们的支付中转站，然而我想说的是事实并非如此。

因此，如果某天闪电网络最终还是为中转站辐射型拓扑网络，那么集中制就是这天中最大的顾虑了。

钱包对钱包的路径

我们可以设计出比中转站辐射型更好的模型吗？现如今已经有很多关于阻止支付中转站的讨论了，人们也在尝试去创造出更分散化、有组织的钱包对钱包的路径。但是这个是如何奏效的呢？试想一下，如果爱丽丝想要买一杯咖啡，在此之前，她的钱包会用相同的技术在网络中通过其他节点找到一个路径来支付这杯咖啡。如果钱包找不到任何一个节点，那么它将与咖啡店打开一个新的支付渠道来完成这笔交易，然后留着这个渠道以便日后再用。理论上说来，爱丽丝的钱包能够维持数十个开放的渠道。

如果有人每次在尝试支付时都不能找到一个渠道，那么新的渠道将会被打开，长此以往用户间的一些有组织的渠道路径就会形成，例如：

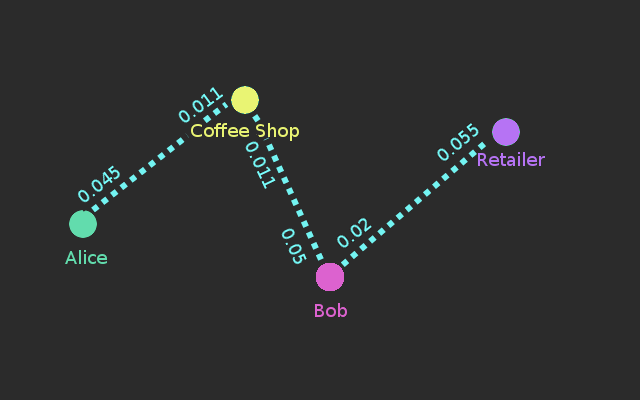


从上图我们可以看到，爱丽丝在离开咖啡店后仍保持其支付渠道的开放，鲍勃最近去了咖啡店后也保持其支付渠道的开放，而且他还从商店里买了一条新领带，这个支付渠道也是处于开放状态。

在这个例子中，爱丽丝不仅可以将比特币以脱链的形式给鲍勃，还可以从已形成的有组织的路径中将比特币付给商店老板。这简直是太棒了！看起来我们似乎已经解决了闪电网络中集中制的问题。但是我们不得不问一下，这种类型的路径可行吗？就我自身而言，我当然希望这是可行的，因为那些比特币的核心开发者们已经把房子都押在上面了。但是当你仔细想一下时，你就会知道这个方法并不切实际。下面我就来阐述一些为什么这个方法不切实际的理由。

当考虑到具体值的情况下，路由路径则是很难被找到的

在上述例子中，我们可以得到一条从爱丽丝到商店并通过咖啡店和鲍勃的路由。现实生活中，它可能很难以我们需要的值来找到一条有组织的路由路径。让我们在我们的例子中添加一些具体值来试试：



爱丽丝和鲍勃都要花5美元来买了一杯咖啡（0.011BTC），这就是为什么咖啡店在爱丽丝和鲍勃的渠道中都有0.011BTC。对爱丽丝来说，不管她是想把钱给鲍勃还是商店老板，咖啡店老板都需要更新他和鲍勃的支付分配渠道，咖啡店老板自己得到的少（从爱丽丝想要付的钱中），鲍勃从中得到的多。但是注意一下，咖啡店老板在和鲍勃的渠道中只有0.011BTC($5)，也就是说爱丽丝最多只能付给鲍勃或是商店老板5$。如果她想要付更多的钱，那她就需要重新开一个新的渠道。

当人们以不同数额的金额买不同的东西时，这种类型的数值不对称性就很有可能会频繁发生。从一个节点到另一个节点的路径是很容易被找到，但是每一次找到正确数值的跳跃路径则是最困难的部分。

最终我们可能使用更多的是链上交易

我们想一下，要是爱丽丝的钱包不能从商店那里找到一条她想要数额的路径时，她是怎样开启一条新的渠道的。据推测，在给定的时间内，你钱包中的比特币，尽管不是全部，也有绝大部分会留在渠道中。那么爱丽丝的钱包哪里还有比特币来和商店开一个新的渠道呢？好，如果它不得不关闭现存的渠道之一，那么当你的钱包在交易时不能找到一条路径的过程将是这样：  
1) 关闭现有的一条渠道来完成上链交易。  
2) 和收款人开启一条新的渠道来完成上链交易。

这两笔上链交易中还只有一笔付款。要是有一笔大交易无法找到一条路径（因此不得不关闭一个旧的渠道来打开一条新的渠道），很多的存款都将被浪费掉。如果有超过百分之五十的交易找不到路径，闪电网络实际上会更多促成的是比特币上链交易，而不是直接付钱给人的交易。

绝大多数的用户会处于离线状态的

在一定程度上来说，人们即便是使用桌面上的钱包，也不会让它二十四小时都挂着，他们在不用钱包的时候就会关闭程序，盖上笔记本电脑的盖子，关掉电脑等。除此之外，很多人的手机钱包都是休眠状态，不会时刻保持上线状态。因此我们否决了这个方案，因为我们99%的预期用户都不会参与路由付款。如果不是之前有组织的路径工作良好，那么99%的预期用户都不会参与的可能性会变得有多小？

渠道无法即时创建

还记得当钱包无法找到路径时，它们会使用魔法般的能力来即时开创出新的渠道。在我们以前的例子中，爱丽丝要给咖啡店付款，她的钱包无法找到路径，于是钱包只能开创一条新的渠道并使渠道一直保持开放状态。

这在过去也许还行得通，但是记住，现在核心开发人员已经给我们增补了全RBF（注意当区块处于满额状态时它不会选择性的加入，它是强制性的加入否则你的交易将会被卡住）。于是你只是不能即时开启新的渠道（至少不能进行零售购买），因为建立渠道的比特币可以被自如地双向使用到其他地方，所以你只有在渠道确认后才能进行付款。因此现在我们留下的是，如果你不能通过现存（已确认）的渠道来找到一条路径，那你就不能向商店老板付款。这将对使用大型已连接的支付中转站产生巨大的压力，因为那是你唯一能保证通过已确认渠道所获得的路径的方法。

接收者必须在线

回想一下以前例子里关于HTLC的路径的解释。爱丽丝的钱包联系鲍勃的钱包，并问它要一个哈希化的随机数字(R)。好吧，基本上鲍勃是需要在线才能将那个数字给她。这个能够直接和比特币进行对比，因为在比特币目前的使用中，发送者和接收者是不需要同时在线的。当然鲍勃可以将这个功能外包给第三方（这简直是一个丢脸的解决方案IMO），但这也正好对只能用一个支付中转站，而不是有组织的路径造成了更多的压力。

所以当我们把上述的所有的点都考虑进去时，这种有组织的钱包对钱包的路径似乎并不能运行得特别顺利，而且对于用原始的中心辐射型模型也会有压力。

考虑到所有的点后（就是已知的核心开发团队），除了等着看到闪电网络是如何发挥作用，你还真没有办法证明那些急于贬低比特币核心功能的对错。如果闪电网络最后不了了之了（当然我们并不希望这个发生），那么比特币就会像我们一样，别无选择，只能以那点来利用它了。