谈一谈：侧链、驱动链和Rootstock双向挂钩设计

**[peterhon](http://www.8btc.com/author/11397" \o "由 peterhon 发布) 2016-04-10 08:41 发布在**[**比特币**](http://www.8btc.com/bitcoin)[**3**](http://www.8btc.com/sidechains-drivechains-and-rsk-2-way-peg-design#comment)**3147**

在最近的技术论文中，我们分析了以不同的方法来实现双向挂钩。在这篇文章中，我们将总结双向挂钩是什么，以及它是如何实现的。



什么是双向挂钩（2-way peg/2WP）

双向挂钩（2WP）允许将比特币从比特币[区块链](http://8btc.com/article-44-1.html" \o "区块链)转移到辅助区块链，反之亦然。“转移”实际上是一种错觉：比特币其实并没有转移，但在比特币区块链上被暂时锁定，而同时在辅助区块链上有相同数量的等价令牌被解锁。当等量的令牌在辅助区块链上被再次锁定时，原先的比特币就会被解锁。这实质上就是双向挂钩所要实现的功能。这一功能的问题是，理论上只有当辅助区块链最终结算时才能被实现。因此，任何双向挂钩系统必须作出妥协并且依靠于假设双向挂钩相关参与者是诚实的。最重要的假设是，主要的区块链是无需审查的，而且大多数比特币矿工都是诚实的。另一个需要的假设可能是，大多数监管锁定比特币的第三方也是诚实的。如果这些假设不成立，则比特币及等效辅助区块链的令牌可以被同时解锁，那么恶意的双花就变得可行了。任何双向挂钩系统都必须选择一种措施，使得被假设要诚实的各方都能在经济和法律方面受鼓励去依章办事。这包括分析这些关键方对区块链网络进行攻击的成本及后果。双向挂钩实施的安全性取决于激励机制，以便参与双向挂钩系统的关键方能够真正执行双向挂钩所应实现功能。

那么，什么不是双向挂钩呢

保税托管合同（BEC）是由[比特股](http://www.8btc.com/bitshares" \o "比特股)（bitshares）提出的方法，若被其他平台采用，就可让比特币（或法定货币）在具有不同令牌的智能支付平台上进行交易。要实现这个方法，发行人需要锁定本地货币债券的量等值或一般高于他们所创造的“比特币”量，然后他们创建欠条并在平台上销售。债券金额使用通过查询平台公告的比特币价格动态调整。显然，这不符合双向挂钩的定义，因为新的“比特币”被创造出来了，而且在比特币区块链上没有等价的锁定比特币。保税托管合同的安全模型通常比双向挂钩弱，因为用户必须信任公告，但公告可能由于没有很高的激励机制而难以保持诚实。也有很少或根本没有经济激励让股票经纪人持有如此庞大具有高度可变性的本地令牌债券。

任何的双向挂钩其实都只是一个投票系统

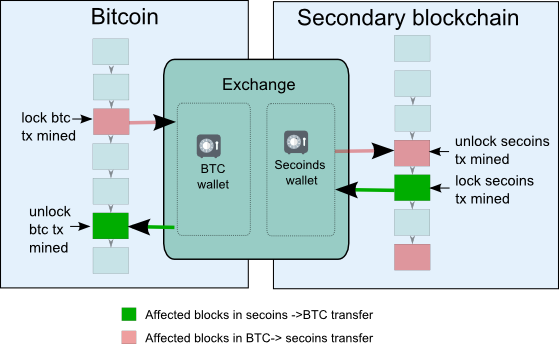
要简化任意双向挂钩的安全模型，我们可以表示为，所有双向挂钩系统都有一组监管人，当辅助链没有达到最终结算时，负责投票何时解锁比特币和发送解锁比特币到何处。投票可以通过数字签名、哈希算力（工作量证明机制）、存储空间（容量证明机制）、加密数字货币控股（股权证明机制）或区块链具有的任何其它共识系统。我们可以改变的每一方投票的权重、投票方的数量、任何一方被允许投票的条件、是否允许投票给一个以上的候选人，如此类推，但我们不能改变的是，该系统本质上是一场投票。

双向挂钩设计

我们将介绍最常见的双向挂钩设计：侧链、驱动链、多重签名保管和混合式设计。为了简化解释，我们将已转移到辅助区块链的比特币称为SE币（secoin）

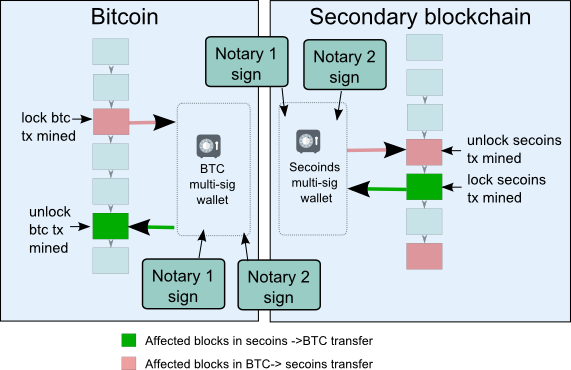
单一监管

一种可能用来实现双向挂钩的选择是，有一个交易所负责监督被锁比特币和解锁的等价令牌。该交易所将在解锁辅助令牌之前实现对比特币的锁定，该过程要么手动执行，要么通过软件协议执行。以下是对这种设置的描述：



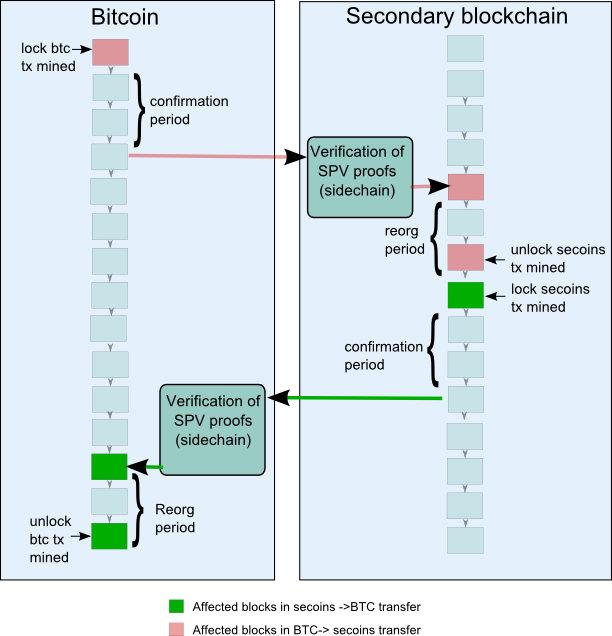
[多重签名](http://www.8btc.com/multisig-the-future-of-bitcoin)联合

实现双向挂钩的一个更好的办法是存在一组掌控多重签名的公证人，他们中的大多数有权解锁资金。这种设置比单一的资金控制者更好，但仍可能导致控制权集中。为了实现真正的去中心化，应慎重选择公证人，因此他们要位于不同的领域、不同的地区，而且都要有良好的信誉及安全性。此外，公证人的数量绝不能太少，但也不能太多。以下是对这种设置的描述：



[侧链](http://8btc.com/topic-sidechain.html)

若要在双向挂钩中尽量不涉及更多的第三方，前提条件是每一区块链执行相关的验证协议，而且协议需要通过协商一致才能确认。每一区块链必须了解其它区块链的共识系统，并且，当接收到其它区块链发出了锁定交易证明时可以自动释放比特币，如这里所示：



不过，使用比特币侧链时存在以下几个问题：

• 大多数公共区块链并没有最终结算。如果辅助区块链没有最终结算，那么比特币区块链就不能确定辅助链上的交易是否已被辅助链网络接受（例如锁定SE币）。其所能得到的只是一个概率保证：更多的工作证明确认这笔交易，意味着它被接受的可能性越大。

• 即使辅助区块链具有最终结算，却没有区块链纠缠，那么辅助链也会面临跟比特币区块链一样的问题。如果有区块链纠缠，那么辅助区块链出块率就不会高于比特币的速率。

• 比特币侧链需要通过软分叉或硬分叉来增加复杂的新操作码。Blockstream的方案目前尚未完整，而且SPV（简单支付验证）的工作证明确认也未解决。

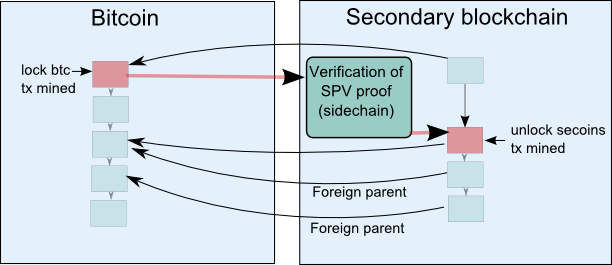
缠结区块链

克服双向挂钩缺乏最终交易问题的一种方法是，缠结区块链，例如主要区块链中的锁定交易的逆转意味着辅助区块链中的解锁交易的逆转。缠结区块链的方式有以下几种：

1. 辅助区块链中的交易被嵌入到主要区块链的交易中（例如，嵌入到OP\_RETURN支付载荷（payload）中，就像合约币（Counterparty）那样）
2. 辅助区块链的区块有两个父块，一个在辅助区块链，一个在主要区块链。辅助区块链节点验证位于主要区块链的父块是否属于比特币的最长链。
3. 辅助区块链的区块由主要区块链交易中的加密监管而锚定。

前面两种方式允许辅助链验证SPV证明无需检验者提供确认标头（header），因为辅助区块链客户端也保存了一份比特币区块链的副本（第一种方式中的整个区块链，且在第二种方式中只需要标头）。而第三种方式并不可行。

下图展示了，通过侧链转移比特币到辅助区块链而无需额外的确认（以比特币可能的最快速度）：

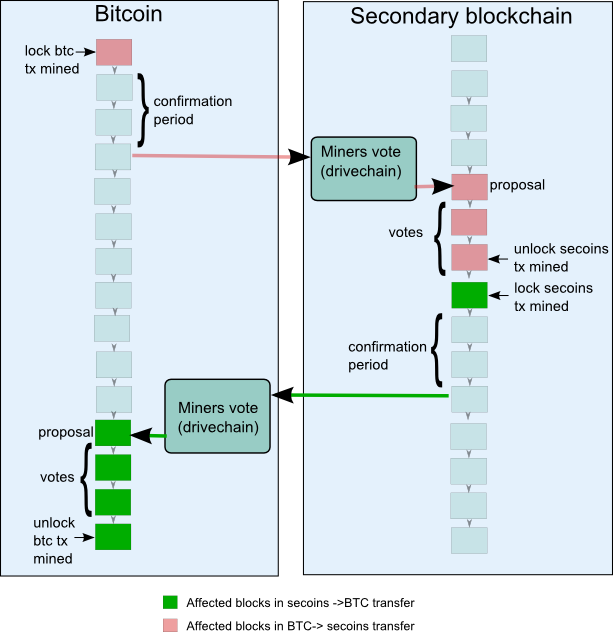


缠结区块链有以下几种缺点：

• 它使得辅助链创建新区块的速率受到比特币区块链限制而较比特币要慢，因为在锚定前，区块链分支的接受情况存在不确定性。难道将已锚定的短链而非较长的未锚定链视为最长链？  
• 当在比特币交易中嵌入辅助链的交易时，辅助区块链的所有用户需要同时处理两条链的交易。  
• 缠结区块链从某一方面解决了最终结算的问题，但并没有解决主要区块链上被锁定的比特币的监管问题。

驱动链

驱动链将被锁定比特币的监管权发放到比特币矿工手上，并且允许比特币矿工们投票何时解锁比特币和将解锁的比特币发送到何处。矿工投票使用比特币区块链，而且是在区块内的某些地方进行投票（例如coinbase）。诚实矿工在驱动链中的参与程度越大，安全性也就越大。下图是对驱动链的描述：



混合型

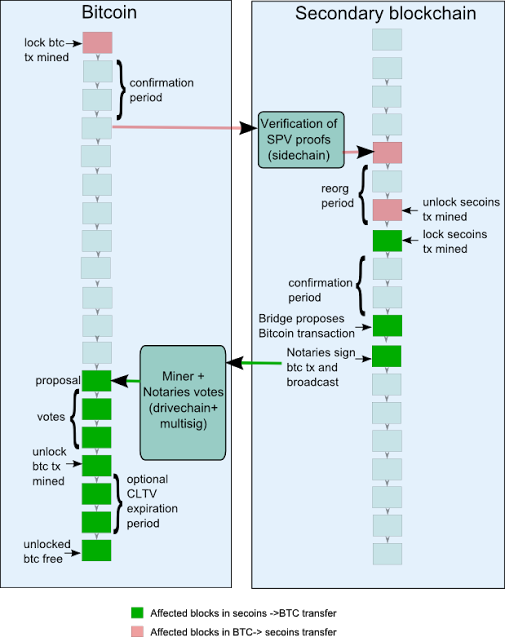
迄今为止所提出的全部设计都是对称的：用于解锁SE币的方法与解锁比特币的方法是相同的。但主要区块链和辅助区块链有本质的不同：主要区块链仍在发行新的本地令牌而辅助链上没有。这在安全性方面存在巨大的隐患，表明了对称的双向挂钩模型可能是不够完善的。混合双向挂钩是对每一边使用了不同的解锁方法，例如在辅助区块链上使用侧链而在主要区块链网络上使用驱动链。

RSK案例

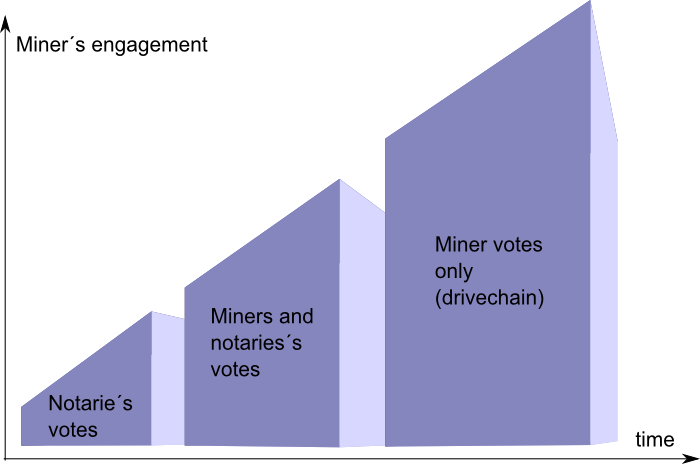
RSK的案例即Rootstock的案例很特别。RSK依靠于一种基本的设计选择：必须允许与比特币联合挖矿。因此，我们必须分析一下这种情况下的最佳设计。我们要考虑到：

• 哪一方控制被锁定的比特币  
• 对区块链网络进行攻击的成本是什么  
• 攻击的后果是什么  
• 这其中的激励机制是什么

如果几乎全体比特币矿工参与到联合挖矿中，我们发现，当监管者是比特币矿工时，参与者才最有可能保持诚实，但只有当几乎所有人都参与其中。在联合挖矿的情况下，驱动链和侧链都完全依靠比特币矿工的诚实，并且都提供相同的安全性。然而，侧链在比特币一侧实现起来要复杂得多，所以对于比特币一侧，RSK的最佳选择是使用驱动链。在RSK方面，我们可以执行侧链的方式。**所以在这一点上RSK的混合模型可以被定义为“驱动链/侧链”。**



当联合挖矿的参与程度低时，“驱动链/侧链”只能提供很低的安全性。因此，我们建议采用一种混合模型，其中被锁定比特币的安全性是基于驱动链加上一组公证人。矿工和公证人（按不同的权重）投票决定解锁哪些比特币。公证人使用他们的数字签名进行投票，而矿工则在他们的coinbase交易中增加一个特殊的标记进行投票。这是中心化和安全性之间的一种权衡。最终的RSK双向挂钩设计可以被定义为“（驱动链 +公证人）/侧链”（前者针对比特币链，后者针对辅助链）。要设置投票的权重，我们使用基于联合挖矿参与程度的动态方法。初期，在传统多重签名交易中只有公证人投票。到了中期，当驱动链功能被添加到比特币时，无论是公证人还是矿工们都将按部就班地投票。从长远来看，当联合挖矿的参与程度达到90％时，公证人将停止投票，而只有矿工会继续投票。这种演变如下图所示：



在本质上，我们建议将被锁定比特币的安全性依赖于矿工和一组公证人，但是这两个投票方之间权力的量是相对于联合挖矿参与量而动态地调整的。

在之后文章中，我们将展示驱动链+公证人的设计是如何在比特币上实现的，其中通过执行单一的操作码OP\_CHECK\_VOTES\_MULTISIG\_VERIFY，这一操作码从概念上理解和实际编程都很简单，并且可以以软分叉的形式在网络上展开。