连载｜侧链白皮书：用楔入式侧链实现区块链的创新—前言续

**[chehw](http://www.8btc.com/author/326" \o "由 chehw 发布) 2014-10-29 09:46 发布在**[**比特币**](http://www.8btc.com/bitcoin)[**14**](http://www.8btc.com/enabling-blockchain-innovations-with-pegged-sidechains-introduction#comment)**4877**

[前文](http://www.8btc.com/enabling-blockchain-innovations-with-pegged-sidechains-abstract-introduction)提到： “比特币系统的目标相对简单：它是一个支持单一原生数字资产传输的区块链，不能与其他任何资产相兑换。这可以简化很多具体实现，不过这样的简化正面临着现实世界需求的挑战”，以及目前比特币系统所进行的一些创新和取舍。以下为续：

－－－－

[](http://7fvhfe.com1.z0.glb.clouddn.com/%2540%252F%2F/wp-content/uploads/2014/10/sidechain1.png)

实际上，由于功能必须被广泛认可后才能采纳，这限制了参与者的个人自由和对其钱币的自主性。小的团体无法实现诸如专用脚本扩展这样的功能，因为他们缺少广泛的共识。

早期针对比特币系统中这些问题的解决方案是可替代的区块链的开发，又称竞争链(altchains)，除针对上述关注点有所修改外，共用了比特币系统的代码库。然而，靠创建一个独立的但本质类似的系统来实现技术变更，是存在问题的。

问题之一是，基础架构碎片化：由于每个竞争链都使用自己的技术堆叠，经常会有重复性或遗失的工作。因此，由于竞争链的实现，可能并未扫除比特币系统中安全特定领域知识的障碍，安全问题常常跨竞争链被复制，而它们的修复也不解决这些问题。必须消耗大量资源或是建立专家评价评审新的分布式加密系统，如果没这样做，安全隐患常常无法察觉，直到漏洞被利用。结果是，我们看到了一种动荡的、无法前航的发展环境，大部分显现出来的项目可能在技术上是最不健全的。打个比方，想象一下在互联网上，每个网站使用自已的TCP实现将自定义的检验和数据包拼接算法广播给最终用户。这不会是一个能生存的环境，这也不是竞争链能生存的环境。

问题之二是，这样的竞争链和比特币系统一样，通常有自己的带有浮动价格的原生加密货币，或称竞争币。为了使用竞争链，用户需要通过一个市场来获取这种货币，这将使他们直接面对新货币带来的高风险和波动。此外，因为有独立解决初始分配和估值问题的需求，与此同时还要在不良的网络效应与拥挤的市场中竞争，这既阻碍了技术创新，又助长了市场的博弈。这危及的不仅仅是这些系统的直接参与者，还危及到整个加密货币行业。如果这一领域被公众认为风险过高，对加密货币的采纳可能会受阻，或者有可能完全被遗弃（自愿或立法上）。这表明我们希望有一个环境来让可互操作的竞争链能易于创建和使用，但不要产生不必要的市场和开发碎片。在本文中，我们认为这些看似矛盾的目标有可能同时实现。核心考察点是 “Bitcoin” 这一区块链在概念上是独立于“bitcoin”这一资产：如果我们能在技术上支持区块链间资产的移动，可以通过简单地复用现有比特币的方式，开发出用户可能会采纳的新系统。

我们称这种可互操作的区块链为“楔入式侧链”。 我们将在第三节中给出精确的定义，这里先列出以下“楔入式侧链”所需具备的属性。

1．在侧链间移动的资产应当能够被当前持有者移回，但除此之外的任何人则不行（包括前持有者）。

2．资产的移动应当无交易对手风险；也就是说，不诚实的一方无法阻止转移的发生。

3．资产转移应当是元操作（原子操作），即，要么完全完成，要么根本不发生。不应存在会导致资产损失或允许欺诈产生的失败模式。

4．侧链应当设有防火墙：一个会使某条链发生资产铸造（或偷盗）的缺陷（bug），不应导致任何其他链出现资产的铸造或偷盗。

5．区块链重组时应当处理干净，即使在资产转移的期间也要如此；任何破坏应当只发生在它所处的侧链上。总的来说，理想情况下，侧链应当完全独立，自其他链上的全部所需数据由用户提供来。侧链的验证者应当只有在侧链本身的显式共识规则有要求时，才需要跟踪其他链。

6．不应要求用户去跟踪他们未主动使用的侧链。

早期“转移”钱币的解决方案是用一个可公开识别的方式来销毁比特币，让新的区块链能检测到，以允许铸造新币［Bac13b］。这解决了部分上面提到的问题，但由于这种方法只允许单向转移，因此还不足以满足我们的目的。

我们提出的方案是由资产转移的交易本身提供所有者证明来转移资产，避免让节点有跟踪发送方链的需求。从上层实现角度，当资产从一个区块链向另一个链移动时，我们在第一个区块链上创建交易锁定资产，然后在第二个区块链上创建一笔交易，该交易的输入中包含一个锁定已正确完成的密码学证明。这些输入用某种资产类型来标记，比如创生出资产的区块链的创世哈希(genesis hash)。

第一个区块链我们称之为父链，每二个则简单称为侧链。在某些模型中，两条链可对称地来处理，因此这一术语应当看成是相对的。从概念上讲，我们打算将资产从（初始）父链转移到一条侧链，可能会再转移到别的侧链，最终还能转回至父链，并保全初始资产。一般我们把父链看成是比特币系统，侧链是其他区块链中的某一个。当然，侧链的币(coin)也可以在侧链间传递，并非只能与比特币系统进行往来；不过，由于任何一个最初从比特币系统移动的币都可以移回去，所以不管变成什么样，它仍是个比特币。

这让我们解决了前面章节提到的碎片化问题，对只想专注于技术创新的开发者来说是个好消息。

此外，由于侧链是从父链中转移现有资产而不是另铸新资产，侧链不会引起未经授权的铸币，维护资产的安全和稀缺性依靠父链来实现。

更进一步说，参与者不必再担心他们的持有物会被一个实验性竞争链锁往，因为侧链币能够用等额的父链币来赎回。这提供了一个退出机制，减少因软件无人维护而造成的损失。

另一方面，由于侧链还是一个独立于比特币系统的区块链，它们可以自由地尝试新的交易设计、信任模型、经济模型、资产发行语义，或加密特性。我们将在第5节中进一步探讨一些侧链的可能性。

这一基础架构的额外好处是对比特币系统本身进行改变不再那么迫切：与其策划一个需要各方均达成一致并一起实施的分叉，不如用侧链来创建一个新的“改变了的比特币系统”。从中期看，如果广泛认可新系统有进步，最终会明显看到，相对于比特币父链，更多的人会使用这个新系统。由于父链的规则没有任何修改，任何人都可以根据自己的时间去切换，不会有任何因共识失败所带来的风险。从长期看，如果父链被认为，或当父链需要改变时，侧链的成功将给父链的更改提供了所需的信心。