连载｜侧链白皮书：用楔入式侧链实现区块链的创新—2 设计原理、3 双向楔入

**[chehw](http://www.8btc.com/author/326" \o "由 chehw 发布) 2014-10-30 09:30 发布在**[**比特币**](http://www.8btc.com/bitcoin)[**12**](http://www.8btc.com/enabling-blockchain-innovations-with-pegged-sidechains-design-rationale-symmetric-two-way-peg#comment)**4654**

 前文为摘要与前言，本文为侧链白皮书连载三，介绍 “楔入式侧链”的设计原理及其技术基础 “双向楔入”（相关定义，对称式双向楔入及整个转移过程，非对称式双向楔入）。

－－－－

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

**2 设计原理**

“无需信任”指的不依赖外部的可信方也可完成正确的操作的特性，一般是能够让所有参与方自己验证信息是否正确。例如，密码学签名系统中，“无需信任”是一个隐式的必要条件（如果攻击者能伪造签名，那么这个签名系统将被视为被完全破解）。虽然分布式系统中一般不需如此，但比特币在系统的大部分中提供了“无信任”操作。

“楔入式侧链”的一个主要目标是在比特币系统模型之上最小化附加的信任。难点是币在侧链间的安全转移：接收链必须能得知发送链的币已被正确锁定。在比特币的领导下，我们提议用DMMS来解决这一问题。尽管有可能利用一个简单基于信任的方案，引入固定数量签名者来验证币的锁定（参见附录A），但有很多重要理由让我们避免这种单点故障的引入：

l信任个人签名者，并不仅仅意味期待他们做事诚实，他们还必须永远不出漏洞、永远不会泄露关键的秘密、永远不会被挟持、永远不会停止参与网络。

l由于数字签名是长期存在的，对任何信任的要求也必须如此。经验告诉我们，即使时间跨度只有几个月，信任需求也是一种危险的期待，更何况我们所期望的金融系统所能持续的时间长达几个世代。

l在比特币系统消除了单点故障前，数字货币一直没有什么吸引力，社区强烈反对引入这种弱点。2007年以来的金融事件更加强了社区的不信任；对金融系统和其他公共机构的公共信任也同样处于历史的低点。

**3 双向楔入**

楔入式侧链的技术基础称作双向楔入。本节我们将解释它是如何工作的，先给出一些定义。

**3.1 定义**

l币(coin)，或资产，是一种可以用密码学方法辨识控制者的数字财产。

l区块，是一个描述资产控制发生变化的交易的集合。

l区块链，是一个有序次的区块的集合，所有用户必须（或最终）对该集合达成共识。这确定了资产控制的历史，提供了一个计算上无法伪造的交易时序。

l重组，或称reorg，发生在客户端本地，当先前已接受的链被一个有更多工作量证明的竞争链取代时，分叉上失败一方的区块要从共识历史中移除。

l侧链，是验证来自其他区块链数据的区块链。

l双向楔入，指的是让币以一个固定或确定性的汇率在侧链间转出和转入的机制。

l楔入式侧链，是一条资产可以从其他链导入并返还的侧链；即，一条支持双向楔入资产的侧链。

l简单支付验证证明（或称SPV证明），是一种动态成员多方签名（DMMS），发生于一条类比特币系统工作量证明(proof-of-work)区块链上。

本质上，SPV证明是由一个展示工作量证明的（a）区块眉列表，和一个（b）表明某一输出发生在列表中的某一个区块的密码学证明所组成。

这使验证者可以检查是否有一定数量的工作已经认可了某个输出的存在。当有其他证明(proof)展示了一条工作量更多的链，且生成该输出区块未包含于其中时，其他证明会使这一证明失效。

使用SPV证明来确定交易历史，隐含着要信任最长的区块链也是最长的正确区块链，在比特币系统中，这是由一个被称为SPV的客户端实现的。由于诚实的哈希算力不会为一个无效链去工作，只有当超过50%的哈希算力合谋时，才会始终欺骗SPV客户端（除非客户端处于长期的女巫攻击之下，使其无法看到实际的最长链）。

还可以这样做，通过获取每个区块眉来指代区块链上未花费输出的集合，任何拥有SPV证明的人不需要“中继”（relay）每个区块也能确定链的状态。（在比特币系统中，完全验证者第一次开始跟踪区块链时需要做这种中继。）

正如我们将在附录Ｂ中讨论的那样，通过在比特币系统的区块结构中包含一些额外数据，我们可以生成比区块眉完整列表更小的证明(proofs)，从而提高可扩展性。尽管如此，这样的证明还是比普通的比特币交易要大得多。幸好对于大多数资产转移来说，这并不是必要的：每条链的持币人可以用附录Ｃ描述的方法直接使用元互换（原子交换）操作［Nol13］进行汇兑。

**3.2 对称式双向楔入**

我们可以利用这些想法将一个侧链SPV楔入至另一个侧链。这包含以下工作：为了将父链币转移为侧链币，父链币被发送到父链上的一个特殊输出中，该输出只能由侧链上拥有的一个SPV证明来解锁。为了在两条链上进行同步，我们需要定义两个等待周期：

１．侧链间转移的确认期，是指币在转移至侧链之前，在父链上必须被锁定的期间。此确认期目的是生成足够多的工作量，让下一个等待期内的拒绝服务攻击变得更困难。典型的确认期的量级可以是一或两天。

当父链上生成了特殊输出后，用户等待确认期结束，然后在侧链上生成一个引用该输出的交易，提供出一个它已被创建并在父链上被足够工作量覆盖的SPV证明，

确认期是一个依侧链而定的安全参数，要在跨链交易速度和安全性间做权衡。

２．接下来，用户必须等待一个竞赛期。这个期间，新转移过来的币不能在侧链上花费。竞赛期的目的是防止重组时出现双花，在重组期间转走先前锁定的币。在这个延迟期内的任何时刻，如果有一个新的工作证明发布出来，对应的有着更多累计工作量的链中没有包含那个生成锁定输出的区块，那么该转换将被追溯为失效。我们称此为重组证明。

只要有可能，所有侧链上的用户都会有动力来制发重组证明，因为对不良证明的承认会稀释所有币的价值。

典型的竞赛期也是一或两天的量级。为了避免这些延迟，用户很可能用元互换（原子交换）(在附录Ｃ中有描述)进行大多数交易，只要有流动性的市场可用。

当币在父链上被锁定时，该币可以在侧链内自由转移，不需要与父链进一步交互。不过，它仍保留着父链币的身份，仅能转回到它所来的那一条链上。

当用户想把币从侧链上转回父链时，与原先转移所用的方法相同：在侧链上将币发送至一个SPV锁定的输出，产生一个充分的SPV证明来表明该输出已完成，使用这个证明来解锁父链上先前被锁定的那个等面值的输出。整个转移过程如图1所示。

|  |  |  |
| --- | --- | --- |
| 父链┆发送SPV锁定的输出等待确认期                竞赛期开始      竞赛期结束（失败）      等待竞赛期  ┆  (链内转移) | SPV证明————————->            SPV证明  <————————-    SPV重组证明  <————————-    新的SPV证明  <————————- | 侧链┆等待竞赛期  ┆  (链内转移)  ┆  发送SPV锁定的输出等待确认期 |

图1：双向楔入协议示例

由于楔入式侧链可能会从很多链中搬运资产，且无法对这些链的安全性做出假定，因此，不同资产不可相互兑换是非常重要的（除非是一个显示声明的交易）。否则，恶意用户可以通过创建一条资产毫无价值的无价值链进行偷盗，将这样一种资产移到一个侧链，再把它和别的东西去兑换。为了应对这种情况，侧链必须有效地将不同父链中的资产处置为不同的资产类型。

总之，我们提议让父链和侧链相互做数据的SPV验证。由于不能指望父链客户端能看到每条侧链，为了证明所有权，用户必须从侧链导入工作量的证明到父链。在对称式双向楔入中，反向的操作也是如此。

为了让比特币系统成为父链，需要有一个能识别和验证SPV证明的脚本扩展。最起码的要求是，这种证明需要做得足够小，以便能放进比特币系统一个交易之中。不过，这只是一个软分叉，对于不使用新功能的交易不会产生影响。

**3.3 非对称式双向楔入**

上节以“对称式双向楔入”作为标题，是因为从父链向侧链的转移机制与反方向的机制是相同：都拥有SPV安全性。

另一种方案是非对称式双向楔入：这种方式下，侧链上的用户对父链能完全验证，由于所有的验证者都知道父链的状态，从父链向侧链的转移不需要SPV证明。另一方面，由于父链并不知道有侧链，所以转回到父链时需要有SPV证明。

这对安全性有所促进，现在，即使一个51%攻击者也没法错误地将币从父链转移到侧链。不过，相应的代价是迫使侧链的验证者去跟踪父链，同时也意味着发生在父链上的重组也可能导致侧链上的重组。在这里，我们不详细探讨这种可能性，因为围绕重组的议题会导致复杂度显著扩大。