连载｜侧链白皮书：用楔入式侧链实现区块链的创新— 附录A 联合楔入

[**chehw**](http://www.8btc.com/author/326)**2014-11-04 18:11 发布在**[**比特币**](http://www.8btc.com/bitcoin)[**2**](http://www.8btc.com/enabling-blockchain-innovations-with-pegged-sidechains-a-federated-peg#comment)**3340**

任何对比特币系统脚本的增强，都可由一个相互间不信任的工作人员组成可信联盟来评估脚本，通过签发一个普通的多重签名脚本来接受。也就是说，这些工作人员充当了协议的适配器，评估那些我们想让比特币系统来做，但因缺乏脚本支持而做不了的相同规则。借助这种方法，我们能够实现一种联合的楔入。

－－－－

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

**附录A 联合楔入**

部署楔入式侧链的挑战之一是，目前比特币系统的脚本在编码SPV证明的验证规则上，还不能完全表达。需要用一种安全、兼容、并且泾渭分明的方式加入所需的表达（例如，通过用软分叉，将一个“无操作”(no-op)指令转化为一个OP\_SIDECHAINPROOFVERIFY指令）。不过，构建共识并部署这样简单的新功能的难度可不小。别忘了这些困难正是楔入式侧链产生的部分起因。我们想要的是，能有一种方法，为比特币系统尝试未来的脚本功能，同时无需在所有地方部署。幸运的是，通过采纳一些用低信任设计目标换取的附加的安全性假设，可以在完全无许可的方式下进行初始部署。

关键的考察点是，任何对比特币系统脚本的增强，都可由一个相互间不信任的工作人员组成可信联盟来评估脚本，通过签发一个普通的多重签名脚本来接受。也就是说，这些工作人员充当了协议的适配器，评估那些我们想让比特币系统来做，但因缺乏脚本支持而做不了的相同规则。借助这种方法，我们能够实现一种联合的楔入。

这种方法与创建一个多重签名链下(off-chain)交易系统非常相似，不过，所需的服务器至服务器的共识处理，借助简单地察看问及的区块链来实现。结果是有了一个确定性的、可审计性高的处理流程，简化了对工作人员的选择和监督。 由于相似性，很多用于提高链下支付系统安全性和可信度的技术，也可以在联合楔入中部署。例如：工作人员地理位置上可以是分散的，通过托管币，或是托管创建成本高的抗协迫的假名身份来进行担保，在有远程证明的防篡改硬件上来实现，诸如此类[Tod 13]。对于小规模的应用，系统中币的所有者自己就可以充当工作人员，从而避免了第三方信任。

一旦带有联合楔入的侧链投入使用，比特币系统脚本附加的SPV验证，可被视为仅仅是一个减少系统中所需信任的安全性升级。现有的侧链可以将币简单地迁移至新的验证系统。这种方法还开启了额外的安全选项：挖矿提供的DMMS对小型系统不是很安全，对大型的系统，联合验证会更危险。侧链可以自适应地并行使用这两种方法，或是根据显见的哈希速率来切换。

考虑一个在工作人员联合体中5取3的侧链实现与比特币系统双向楔入的例子。联合体有secp256k1公共点（公钥）P1、P2、P3、P4和P5以及一个赎回模板，这些对侧链中所有参与者均可见。要将币发送到一个脚本公钥（ScriptPubKey）SPK时，想让币在一个使用联合楔入的侧链上可用的用户，可以依照下面的密钥推导方案，计算跨链P2SH［And12a］地址：

算法1 生成跨链地址

输入：一个将从其他链接收币的目标脚本公钥SPK

输入： 一个工作机关公共点的列表 {Pi}ni=1

输入：一个赎回脚本模板，表述工作机关的需求

输出：一个P2SH地址

输出：用于本实例的临时数（Nonce）

1: nonce ß random\_128bit()

2: for i ß [1;n] do

3: Tweaki ßHMAC-SHA256(key = Pi, data = nonce||SPK)

4: if Tweaki >= secp256k1\_order then

5: Go back to start.

6: end if

7: PCCi = Pi+G×Tweaki

8: end for

9: address ß P2SH\_Multisig(template;keys = PCC))

这个推导方案基于BIP32中使用的同态技术[Ｍax11]，允许第三方导出公开的不可链接的地址。与一个支付到合同（pay-to-contract）交易（GH12）的基础构建相同。产生地址后，可以将币支付到其上，通过将临时数、脚本公钥和一个SPV证明提供给工作人员，使其可以在区块链上找到这一支付，用户随后可以在侧链上收到支付过来的币。为了帮助侧链上的第三方验证，这些数值可以包含于该侧链本身。由于币的转移是通过支付给一个标准的P2SH地址实现的，且可以支付给任何脚本公钥，所有支持支付到多重签名地址的比特币系统服务将立即能支付给，或从使用联合侧链的用户处收到支付。

联合楔入方法需要对信任有所让步，不过不需要比特币系统作改变——仅参与者需要同意使用该方法，并且只有参与者承担使用它的代价或风险。此外，如果有人想阻止其他人使用侧链，他们是做不到的：如果联合楔入在一个封闭的社区私人使用，可以让它的使用无法被检测并且无法被审查。这种方法可以允许快速部署和实验，还将允许在对比特币系统协议采用任何更改前，使社区从楔入式侧链中获得信心。