连载｜侧链白皮书：用楔入式侧链实现区块链的创新— 4 缺陷、5 应用

**[chehw](http://www.8btc.com/author/326" \o "由 chehw 发布) 2014-10-31 09:30 发布在**[**币头条**](http://www.8btc.com/featured)**,**[**比特币**](http://www.8btc.com/bitcoin)[**11**](http://www.8btc.com/enabling-blockchain-innovations-with-pegged-sidechains-drawbacks-applications#comment)**4287**

本文为侧链白皮书连载四，介绍侧链本身的缺陷（复杂度，欺骗性转账，挖矿中心化的风险，软分叉风险），并附解决或变通方案。以及探讨侧链面向用户的应用（竞争币实验和资产发行） ，以有效地扩展比特币系统做它目前还不能做到的事。

－－－－

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

4．缺陷

侧链给加密货币领域中的很多问题提供了解决方案，为比特币系统的革新带来数不清的机会，但同时，侧链本身也并非没有缺陷。本节我们将审查一些潜在问题，并附以解决方案或变通方案。

**4.1 复杂度**

侧链在以下几个层面引入了额外的复杂度。

在网络层面，我们有了许多独立的、非同步的区块链，支持相互间转移。它们必须支持可被后期重组证明宣布失效的交易脚本。我们还需要软件自动检测不正当行为，以及生成并发布相关的证明。

在资产层面，简单的“一条链，一种资产”准则不复存在了；单条链可以支持任意多的资产，甚至包括该链首次被创建时还不存在的资产。这些资产的每一个都要标记上该资产的来源链，以确保资产的转移可以被正确地解析。

仅让区块链基础架构能处理高级功能是不够的：管理钱包的用户界面也需要重新考虑。目前，在竞争币的世界中，每条链都有自己的钱包，用以支持该链上币的交易。需要改写这些钱包以便支持多个链（可能带有不同的功能集）和链间资产的转移。当然，如果令用户界面过于复杂，完全可以选择不使用某些功能。

**4.2 欺骗性转帐**

理论上，任意深度的重组都是有可能的，这让攻击者能制造一个比发送链的竞赛期时间长的重组、在发送链撤消该半侧的转帐前，将币在侧链间完全转移。结果将使接收链上币的数目与发送链上可赎回的锁定输出的数量不对等。如果允许攻击者将币转移回初始链，他将增加他自己币的数量，让该侧链上其他用户付出损失。

在讨论如何处理这一问题前，我们注意到，通过简单地延长转移的竞赛期就可以使这种风险变得任意小。那好，可以用两条链的相对哈希算力生成一个函数来决定竞赛期的持续时间：接收链可以仅在见到一个等同于该链１天工作量的SPV证明时才解锁币，这一证明可能相当于发送链上几天的工作量证明。类似这样的安全参数是特定于侧链的属性，可以针对每个侧链的应用进行优化。

不管这种事件有多不可能发生，很重要的一点是，不能因侧链的责任造成灾难性故障。可以创建一个SPV证明见证这一事件，并且侧链可以接受这种证明。可以设计侧链，选下面的多种方式之一来作应对：

l不做应对。这样做的结果是，该侧链是一个 “部分准备金（银行）”, 存储来自其他链上资产。对于微量数额，如果人们认为少于丢失的侧链币，或是有承保人承诺偿付丢失的资产，这一方式可以被接受。然而，超出一定的阈值后，很可能发生从该侧链提现的“银行挤兑”，最终要有人担下损失。间接损害可能包括对侧链信心的普遍丧失，父链的代价则是要处理一个突如其来的交易高峰。

l楔入及所有相关的交易可以被回退。然而，由于币往往会散发出去，交易历史会交织在一起，即使是刚经历很短的时间就回退，后果也可能是毁灭性的。这还限制了资产的可置换性，接收者将倾向于选择历史“清白”的币（没有近期楔入的）。我们预计这种可置换性的缺失可能会导致灾难性后果。

l所有币的数量可以被缩减，同时汇率维持不变。与新用户相比，在攻击发生前将币转移到侧链的用户会比较不利。这等同于降低侧链币兑换的汇率。

在这些应对基础上也可以加以变化：例如，临时降低汇率，使那些在该侧链“挤兑”的人得不偿失。

**4.3挖矿中心化的风险**

一个重要的顾虑是，引入带有矿工费的侧链是否会给矿工资源带来压力，产生比特币系统（挖矿）中心化的风险。

由于矿工们收到的报酬，来自于其所工作的各链的区块补贴及交易费，出于经济利益，他们会根据难度变化和市场价值变动，切换到价值上差不多的不同区块链，为之提供多方成员动态签名（DMMSes）。

我们的答复是，一些区块链已稍稍改进了区块眉的定义，使其中包含一个比特币系统DMMS，因而，矿工能把提交给比特币系统的DMMS同样用于一个或多个其他区块链——这称为合并挖矿。因为合并挖矿允许将工作量复用到多个区块链上，矿工可以从每个他们提供了DMMSes的区块链上索取报酬。

由于矿工们要为更多的区块链提交工作，跟踪和验证全部这些链需要更多的资源。只为区块链的某一子集提交工作的矿工得到的报酬，比为所有可能的区块链都提交工作的矿工少。小规模的矿工可能无法支付为每个区块链挖矿的全部成本，因而与较大的有组织的矿工相比，会处于劣势，后者能从更大的区块链集合中索取更多的报酬。

不过，我们注意到，矿工们可以将其所工作的任何区块链子集上的验证和交易选择委派出去。选择委托机构能使矿工免除几乎所有对额外资源的需求，或者能为仍处于验证过程的区块链提交工作。然而，这种委派的代价是区块链上验证和交易选择的中心化，即便工作量生成本身仍是分布式的。不过，矿工们也可以选择不为仍处于验证过程的区块链工作，用自愿放弃一些报酬来提高验证过程的去中心化。

**4.4 软分叉风险**

比特币系统中，软分叉是对比特币协议的一个补充，通过在设计上严格缩减合法交易或区块的集合来实现向后兼容。软分叉的实现只需挖矿算力中的绝大多参与即可，不需要所有的完全节点都参与。不过，对于软分叉出来的功能，除非所有完全节点都升级，否则参与者的安全性仅是SPV级。软分叉已经被使用过很多次，用于部署新功能和修复比特币系统中的安全问题（参见[And12b]）。

按本文所述方法实现的双向楔入仅有SPV安全性，因此，对矿工诚实性的短期依赖度高于比特币系统（参考4.2节中所述的攻击）。不过，如果双方系统的所有完全节点都相互检查，并用一个软分叉规则要求相互的合法性，那么，双向楔入的安全性可以提升至完全等同于比特币系统的水平。

这种方式的负面影响是，失去了对任何有软分叉需要的侧链的隔离。由于隔离是使用楔入式侧链的目标之一，除非某一侧链已经几乎被普遍使用，这种结果将是不受欢迎的。不过，假设没有楔入式侧链，接下来的备选方案是直接对比特币系统硬分叉来部署单个的变更。这会更唐突，无法提供真实的机制证明新功能成熟，还需要冒比特币系统共识上的风险。

**5 应用**

抛开技术基础，本节我们探讨侧链的面向用户的应用，这些应用可以有效地扩展比特币系统做它目前还不能做到的事。

**5.1 竞争链实验**

第一个应用，前面已经提及多次，就是简单地创建一条竞争链，该链上币的稀缺性由比特币系统来提供。通过利用一条不用全新货币，而是承载比特币的侧链，避免了初始分配、市场脆弱性、以及新用户接纳障碍等棘手问题，新用户不需要再去找寻值得依赖的市场，或投资于挖矿硬件以获取竞争币资产。

**5.1.1　技术实验**

由于侧链在技术上仍是完全独立的链，它们能改变比特币系统中诸如区块结构或交易链等功能。下面例举一些这样的功能：

l通过修复不期望有的交易可锻性——在比特币系统中只能被部分修复［Wui14］——可以更安全地执行与链上未确认交易相关的协议。交易可锻性是比特币系统中的一个问题，会让随便一个用户以某种方式微调交易数据，尽管交易的实际内容并未发生改变，但依赖于它们的后续交易会遭到破坏。概率性支付［Cal12］就是一例可被交易可锻性破坏的协议。

l提高支付者的隐私性，例如Monero（XMR）中使用的环签名方案，可以减少特定方的交易被审查的系统风险，保护加密货币的可置换性。Maxwell、poelstra[MP14, Poe14b]和Back[Bac13a]对此提出的改进能容许更高的隐私性。目前，可以用Menora币来使用环签名方案，但比特币不能使用；侧链将会避免这种排它性。

l在比特币系统中提出过的脚本扩展（例如，对彩色币[jl213]的有效支持）。由于这样的扩展仅仅对小范围的用户有用，但使所有用户都要因此而应对提高了的复杂度和不易察觉的交互影响造成的风险，因而这些扩展在比特币系统中没被接受。

其他建议的扩展包括对新的密码学原语的支持。例如，兰波特（Lamport）签名，虽然大，但安全性可以对抗量子计算机。

l多种用不兼容的方式扩展比特币系统的想法在［Max14］和[http://www.bitcoin.ninja](http://mail.qq.com/cgi-bin/mail_spam?action=check_link&spam=0&url=http%3A%2F%2Fwww%2Ebitcoin%2Eninja). 中有说明。

由于这些变革影响的只是币的转移，而不是币的铸造，没必要为它们准备一种独立的货币。使用侧链，用户可以安全地、临时性地尝试这些变革。这促进了对侧链的采纳，与使用一种完全独立的竞争币相比，采用侧链时，参与者的风险更小。

**5.1.2　经济实验**

比特币系统的奖励机制是把新币分配给矿工。这实际上使货币膨胀，不过，它会按一个阶梯式时间表随时间推移而逐步下降。用这种通胀来补贴挖矿是对交易费的一个成功补充，用以保障网络安全。

在侧链上获取区块奖励的另一种机制是滞期费，这是由Freicoin（http://freico.in）首创的用于数字货币的一个想法。在滞留型（demurring）加密货币中，所有未花费的输出将随时间推移而减值，减少的价值被矿工重新采集。这在保证货币供给稳定的同时，还能给矿工奖励。与通货膨胀相比，这或许能更好地与用户利益保持一致，因为滞期费的损失是统一制定并即时发生，不会像通胀那样；它还缓解了因长期未使用的“丢失”币以当前价起死回生可能给经济带来的冲击，在比特币系统中这是一种能意识到的风险。滞期费建立了提高货币流通速度和降低利率的激励机制，这被（例如Freicoin的拥护者和其他西尔维奥・格塞尔利息论的支持者[Ges16]）认为对社会有益。在楔入式侧链中，可以用已有价值的货币将滞期费支付给矿工。

其他与经济相关的变革，包括所需的矿工费、交易可逆性、当输出达到一定的币龄就简单地将其删除、或者是将通胀率／滞期费率楔入至侧链外的事件。所有这些变革都很难安全地来进行，不过，由于侧链易于创建并降低了风险，这给变革提供了必要的可行环境。

**5.2　资产发行**

在这一点上，大多数情况下，我们认为侧链不需要自己的原生货币：所有侧链上的币最初都被锁定，直到来自其他某条侧链的资产转入将其激活。不过，侧链也可以制造自已的代币，或是带有自己语义的资产发行。它们可以被转移给其他侧链来换取其他的资产和货币，整个过程不需要对中心方有信任，即使将来赎回时对可信方有需求。

资产发行链有很多应用，包括传统的金融工具，如股票、债券、凭证和白条等。这使得外部协议可以将所有权及转帐记录跟踪等授权给发行所有者股份的那条侧链。发行资产链还可支持更多的创新工具，如智能财产。

这些技术还可在补充性货币［Lie01］中使用。补充性货币的例子包括：社区货币，设计目的是优先推动当地企业；企业易货协会，支持教育或老年护理之类的社会方案；限定用途的代币，在组织机构内部使用，比如大型多人游戏、客户忠诚度计划、在线社区。

一个合适的脚本扩展系统和一个资产可识的交易，能从良好审计的组件中，创建出有用的交易，比如将一个出价和报价合并为一个汇兑交易，能为资产交换以及无信任期权（FT13）这样的复杂合同创建完全无信任的点对点市场。这些合同可能会有所帮助，例如减少比特币本身的波动性。