连载｜侧链白皮书：用楔入式侧链实现区块链的创新— 6 发展方向、7 致谢

[**chehw**](http://www.8btc.com/author/326)**2014-11-03 09:29 发布在**[**比特币**](http://www.8btc.com/bitcoin)[**12**](http://www.8btc.com/enabling-blockchain-innovations-with-pegged-sidechains-future-directions-acknowledgements#comment)**3142**

 侧链中值得探讨的其他一些想法有：保证合同，时移交易费，滞期费，补贴，合签SPV证明，SNARKs，关于低价值或实验性侧链的一个未来想法是，起用一个可信机构……

－－－－

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

**6 发展方向**

6.1 哈希算力攻击抗性

本文的主旨围绕使用SPV证明的双向楔入，它可被一个51%的多数方所伪造，不过也可以区块化，需要大量的哈希算力以便在传输的竞赛期构建一个足够长的证明（后面这一点上要有所权衡——比如，假设33%的哈希算力能使区块出一个证明，那么，要想成功使用一个假证明则需有67%的算力，依次类推。）

侧链中值得探讨的其他一些想法有：

l保证合同。将侧链的交易费扣留，不支付给矿工，直到他们的哈希算力至少相当于比特币系统的，比方说是，66%的算力。加密货币实现这类合同很容易，只要它们最初就设计成这样，用于提高区块转移的成本。

l时移交易费。矿工们的部分交易费要在将来的某个区块中才能收到（或分散到许多区块），使他们有动力来维持链的运作。

这可以激励矿工，使其简单地收到“带外”（out-of-band）交易费（译者注：在传送过程中，不通过常规方式，无需排队（in-band）优先传送给用户，以便及时处理的方式称为out-of-band），避免需要等待将来才能给的链内奖励。该方案的变体是让矿工收到一个令牌（token），允许其将来挖一个低难度值的区块；这个效果是一样的，只不过更直接地激励其接收者来挖这条链。

l滞期费。区块补贴可以通过滞期费形式支付给矿工，以激励诚实挖矿。由于可被转入到比特币系统或其他侧链的数量只能与转出的数量相同，这种基金的重分配将限定在其所发生的侧链之内。

l补贴。侧链也可以发行自己独立的原生货币作为奖励，有效地形成一种竞争币。然后，这些币将有一个自由浮动的价值，结果是无法解决与竞争币相关的波动性和市场碎片等问题。

l合签SPV证明。引入一个必须在合法SPV证明中签字的签名者，对假证明进行监察。这导致要在中心化和抗高算力攻击的安全性间直接做出权衡。在这方面有很大的权衡余地：可以仅在高价值的转移中才需要签名者；仅当侧链的哈希算力过小，只相当于比特币的一个百分比时才需要他们；等等。在附录A中包含有对此类权衡的实用性的进一步讨论。

lSNARKs。密码学学术上的一个令人振奋的近期进展是SNARKs[BSCG+13]的发明。SNARKs是空间效率高，可快速验证计算工作已完成的零知识密码学证明。然而，目前它们的使用是受限制的，因为对于大多数程序，用当今的计算机来生成这些证明的速度太慢，且现有的构建需要一个可信设置，这意味着系统的创建者有能力制造假证明。

关于低价值或实验性侧链的一个未来想法是，起用一个可信机构，该机构的唯一任务是为SNARK方案执行一个可信设置。这样，可以构建区块，证明对未花费输入集合的变更，不过，这是在对实现交易零知识的前提下完成的。这些区块还能对所有先前的区块提交完整验证，允许只验证一个最新的区块，使新用户得到速度上的提升。通过根据一些先前定义的规则证明发送链的合法性，这些证明还可以取代将币从一条链移至另一条链的DMMSes

**7 致谢**

我们要感谢加文・安德烈森、科琳娜・Dashjr、马蒂亚斯・Dybvik、丹尼尔・Folkinshteyn、伊恩·格里格、Shaul Kfir，midnightmagic、帕特里克・Strateman、Kat Walsh和Glenn Willen的审稿意见。