区块链 作业四

> TRY 计算机科学与技术

1.SPV的定义

SPV（Simplified Payment Verification，简单支付验证）是现有区块链互操作性技术中面向加密货币的侧链协议中的CCC协议的典型例子——双向锚定技术(Two-way peg)的其中一类。具体来讲，SPV是比特币中"轻节点"用来验证交易的技术，是原始比特币白皮书中所概述的一个系统，它使轻客户端（在低端系统上运行的钱包）能够验证一笔交易已被打包进入比特币区块链中，以此验证一笔支付的真实性。值得注意的是，不同于"交易验证"，"支付验证"比较简单，只验证这笔交易是否已经存在，即只判断用于"支付"的那笔交易是否已经被验证过，并得到了多少的算力保护（多少确认数）。

2.SPV的作用

SPV能够以**较小代价**判断某个支付交易是否已经被验证过（存在于区块链中），以及得到了多少算力保护（定位包含该交易的区块在区块链中的位置）。SPV 客户端只需下载所有区块的区块头（Block Header），并进行简单的定位和计算工作就可以给出验证结论。主链设立一个特殊的地址，将主链的币发送到该地址以将其锁住，然后将SPV证明传到侧链，侧链释放等值的侧链币。

使用场景如下：

1. 轻钱包中的支付校验
2. 侧链的双向挂钩中，主链和侧链需要通过对某笔特定的交易做SPV验证，以确保该笔交易确实发生过支付，好使得一方锁定资产，一方转移资产。

   a）当用户要向侧链转移比特币时，首先在主链上创建一笔特殊的交易，待转移的比特币被发往一个被锁定的输出，锁定比特币；

   b）等待一段确认期，使得上述交易获得足够的工作量确认 （SPV证明）；

   c）用户在侧链中也创建交易来提取比特币，需要在这笔交易的输入指明上述主链被锁定的输出，并提供足够的SPV证明；

   d）等待一段竞争期，防止双花；

   e）这样比特币就在侧链上自由流通了；

   f）当用户想让比特币返回主链时，采用类似的动作。即先在侧链创建交易，待返回的比特币被发往一个被锁定的输出，等待一段时间确认期后，在主链用足够的对侧链输出的SPV证明来解锁最早被锁定的输出。等待一段竞争期，主链的比特币被解锁，恢复流通。

3.SPV对区块链的利弊

- **好处**：对于只有基本的比特币投资及消费支付需要的普通用户来说，他们没有矿机或高端配置的电脑，无法运行全节点程序。而SPV证明节省了超99.99%的存储空间，使得他们可以在低端设备或智能合约中进行验证。
- **弊端**：
  - 由于SPV没有全部的交易记录，不能验证某个交易不存在，这个漏洞会被针对SPV节点的拒绝服务或者双重支付攻击利用。 例如：如果成功对加密货币进行51%攻击，攻击者就能够骗过

依赖于SPV证明的客户端，使其接受所有的无效交易，比如伪造货币的交易。若成功，就有可能出现双花，从而打破基础的安全假设，对整个系统造成危害。

- SPV节点需要随机链接多个节点，增加与至少一个可靠节点相连接的概率，但是这种随机链接的需求也会容易受到网络分区和sybil攻击。
- 隐私泄漏。SPV钱包仅向SPV钱包拥有的密钥请求来自完整节点的交易，整个节点链接地址和关联交易，使得比特币用户的匿名化变得微不足道。虽然已经尝试用Bloom过滤器来修复SPV隐私，但这种尝试在很大程度上是无效的。如果没有通过诸如Tor的匿名网络发送交易请求，则完整节点不仅会通过一些方式得到SPV钱包相关的特定地址，还会得到SPV钱包的IP地址。