SPV

18308045 谷正阳

1 SPV 的定义

1.1 区块结构

每个区块是包含区块头和区块体的，所有的交易都存在区块体中，而区块头仅记录用区块体的全部交易计算的 Merkel 树根。因此验证区块体有没有被修改，只需要验证 Merkel 树根是否和区块头记录的一致。而整个区块链就是由区块，使用区块头的哈希指针串接而成的链表。

1.2 SPV

SPV 是一种简化的支付验证过程。它的验证过程如下：

1. 节点从区块链网络上获取并存储最长链的所有区块头至本地；
2. 计算待验证支付的交易哈希值；
3. 节点从区块链获取待验证支付对应的默克尔树哈希认证路径；（这里找到了该交易对应的哈希值）
4. 根据哈希认证路径，计算默克尔树的根哈希值，将计算结果与本地区块头中的默克尔树的根哈希值进行比较，定位到包含待验证支付的区块；（找到这个哈希值属于哪个区块）
5. 根据该区块头所处的位置，验证该区块的区块头是否已经包含在已知最长链中，确定该支付已经得到的确认数量，如果包含则证明支付真实有效。（证明本交易得到了 6 次确认）

2 SPV 的作用

SPV 不使用在本地存储全部的区块链，来验证交易的真实存在性，即验证交易已经被 6 次确认过已经被最长链承认了。用它可以实现安装在移动设备上的钱包软件（SPV 钱包，仅提供支付确认而非挖矿）。

另外 SPV 还可以实现双向锚定技术（可以实现暂时的将数字资产在主链中锁定，同时将等价的数字资产在侧链中释放，同样当等价的数字资产在侧链中被锁定的时候，主链的数字资产也可以被释放）进而实现侧链技术。具体来说，SPV 可以证明一个交易确实已经在区块链中发生过，进而实现主链侧链的交互。

3 SPV 对区块链的利弊

3.1 利

SPV 由于最多只需要存储全部的区块头，而不需要存储区块体，可以减小空间开销，因而得以实现部署在移动设备上的 SPV 钱包。另外它也是两条链交互的过程，可以用来实现侧链技术。

3.2 弊

主要是安全性的问题。但是 SPV 因为没有保存全部区块的节点信息，需要和其他节点配合才能进行验证，所以一旦 SPV 节点连入了一个虚假的网络中的，存在被恶意攻击的风险。另外 spv 由于没有全部的交易记录，不能验证某个交易不存在，因而其易受双花攻击的影响。