区块链第四次作业

- 米家龙
- 18342075
- 计算机学院

SPV 的定义

简单支付验证（简称SPV）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。

SPV 有什么用

- SPV 能够以较小的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 客户端只需要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。
- SPV证明节省了超99.99%的存储空间，使得我们可以在低端设备或智能合约中进行验证，但如果要下载每个区块的数据，低端设备是完全无法做到的，从而大大拓展了区块链的使用范围。

SPV 对区块链的利弊

利：

- 使用SPV简单支付验证，可以节省一大笔存储空间，帮助节省更多的硬件控件，拓展了区块链的应用范围

弊：

- 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51%攻击成功，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。