当中本聪使用默克尔树而不是列表来组织交易数据之后，就可以把交易数据从区块链的链式结构中剥离出来，而只把默克尔树的树根，也称作“默克尔根”(Merkle root)，“种在”区块链的区块头里，从而受到区块头中的工作量证明的保护和固定。整个比特币区块链的链式结构中的每一个区块的区块头，都种了一棵默克尔树。每一棵默克尔树的叶子上，都挂着一笔比特币交易。

这样一来，我们就可以把交易数据完全拿掉，只保留链式结构和一棵棵的默克尔树。这样的客户端就可以无需运行一个出块和记账的全节点，也可以验证付款。“他无法自行检查交易，但是通过把这笔交易关联到链的某个位置，他就能看到一个网络节点接受了这笔交易，在此之后新增的区块进一步确认网络已经接受了该交易。”中本聪在2008年比特币白皮书的第8小节中如此写道[1]。第8小节的题目叫做“简单支付验证”(SPV, Simplified Payment Verification)。

由于区块头的数据相比完整区块小了很多，甚至可以在移动设备比如智能手机上装下整个区块链。采用了简单支付验证技术的客户端也叫做SPV钱包，或者轻量级钱包。

在2008年11月3日的邮件里，中本聪解释说，“在网络变得很大之前，用户就可以安全地使用“简化支付验证”（第8节）来检查双重花费，这只需要拥有区块头的链，每天大约12KB。只有尝试铸币的人才需要运行网络节点。最初，大多数用户都将运行网络节点，但是随着网络的增长超过某个特定点，只会剩下拥有专用硬件机场(server farm)的专家才会运行(网络节点，即挖矿记账节点)。一个机场只需要在网络上有一个节点，而其余的节点则可通过局域网与该节点连接。”[2]

在2010年5月18日的论坛帖子中，中本聪进一步解释，“简单支付验证为轻量级客户端用户而生，这些客户端只做交易转账，既不挖矿也不参与到节点网络中。他们不需要下载区块，只需下载哈希链，哈希链当前约为2MB，验证速度非常快（验证整条链少于一秒钟）。如果网络变得非常大（例如超过100,000个节点），这就是我们将要采用的技术，用来允许普通用户进行交易，而无需成为全节点。到那个阶段，大多数用户应该开始运行只做客户端的软件，只有专业机场才能继续运行完整的网络节点，就像usenet新闻组网络的合并一样。”[3]

“该设计概述了不需要完整区块链的轻量级客户端。在设计文档中，它称为简化支付验证(SPV)。轻量级客户端可以发送和接收交易，只是不能创建区块。它不需要信任节点来验证付款，它仍然可以自己验证付款。”中本聪在2010年7月14日的论坛帖子中继续写道。

“我预计不会有超过10万个节点，可能更少。它将达到一个平衡，在该平衡下，不值得再有更多的节点加入。其余的将是轻量级客户端，可能有数百万。”中本聪对

于比特币网络规模的估计，比特币用10年时间完成了1/10，达到了1万个左右的分散在全球各处的全节点。

中本聪继续写道，“在平衡大小下，许多节点将是具有一个或两个网络节点的机场，这些网络节点通过局域网为机场的其余部分投喂数据。”