# 深入浅出比特币签名（2）

**等一轮残月** 管理员 船龄 **7.1年** 2016-03-02 10:03:00 来源 **巴比特论坛**



http://8btc.com/thread-29772-1-1.html

之前这个贴说过，签名就是拿私章盖在一串数12345上，那这是串什么数？

了解这点之前，先看一下原来的交易乙，这里汇款信息一侧是由签名和公钥B组成，但实际上在比特币里，这部分信息虽是主要的，但并不是全部，有些附加信息我一开始略掉了，这里加上，可以看到有数字13524, 47，41，88，ac 等等。。。13524是前一个交易的总笔画数（哈希值），用于验证花的币所在的前一个交易是正确的，而47，41之类数字可称为会计操作流程，比特币中叫做脚本（script）

会计操作流程是怎么回事？

从安全角度考虑，我们假设审核这些交易的会计（全节点）都是些小学文化的只懂按计算器和验证的人。所以具体如何验证这些交易，我不把任务交给会计，而是要求她们全部照章办事，这个章程就是会计操作流程。她们每个人都有一本小册子，里面有80条会计操作流程，有些很简单就是一步的操作（比如说47），有些较复杂，有多步的操作（比如说ac）。但无论如何，她们只需按汇款单上写的操作流程来做就行了

这样做的好处在于，我在汇款单上可自定义操作流程来实现一些扩展的功能，而不需要每次一想实现新功能都要重新给会计培训（升级全节点），比如实现多重签名（会计必须验证3个签名中的2个才判定交易合格），比如实现智能合约（会计必须收到其他传真才能判定交易合格），等等。。。

顺便提一下以太坊(Ethereum)。以太坊和比特币的根本区别，就在于这些操作流程上。中本聪设计比特币的时候，特意让这些操作流程极为简单，不能实现很复杂的功能，他认为一个货币体系的主要功能就是转账，这些会计不该什么事都做。但以太坊则不同，就是把这套操作流程编的非常繁复，功能非常强大，形成了一整套计算机语言。也就是说以太坊主要是利用区块链来实现非转账的其他功能，那种情况下，就不是汇款单，可能是合同，条款等等，让职员来根据以太坊的操作流程判断合同是否可以执行

当然了，虽说操作流程可随便组合，但在比特币中绝大多数情况下都是只有一种操作流程即P2PKH，也就是验证私钥签名，即本例中的内容

会计拿到汇款单（交易乙）后，具体操作流程如下：

第一步，先从付款信息取出要处理的部分：

1. 取那串数字12345和上面的签名部分
2. 取公章B

这两个操作（比特币中代码47和41）是写在付款信息里的，47是指取签名总长47位，而41是指取公钥的总长41位。会计一看到47就知道是取数字加签名，一看到41就知道是取公钥

第二步麻烦一些，从前一个交易（交易甲）的收款信息里找到如何验证交易（按照交易甲的兑现条件来操作，但可以参考交易乙的收款信息，操作代码是一样的）



下一篇：**什么是公共区块链（公链）？**

1.数公章B的总笔画数 （a9）
2.取地址B （14 地址B）
3.验证公章B的总笔画数是否等于地址B，不相等则交易无效 （88）
4.验证那串数字12345上的私章是否和公章B的裂缝吻合，不吻合则交易无效 （ac）

这里的第四步，那串数字12345已跟私章混在一起无法辨认了，会计需要重新构造这串数字，然后用公章盖上去，再和原来私章盖上去的图像对比，以验证私章的有效性

这串数字12345怎么构造呢？是根据数交易乙里所有字的总笔画数来构造的

这就出现了一个逻辑问题：要数交易乙的总笔画数（算哈希），我必须连付款信息中的这串数字和盖在上面的私章都一起数，那在还没有这串数字和私章的时候，我怎么知道交易乙里的总笔画数呢？

因此，中本聪是这样设计的：交易乙的付款信息中先用铅笔填上前一个交易的收款信息（也就是交易甲里的金额，地址B，兑现条件），然后来数交易乙的总笔画数（假设得到12345）

对乙来说，他要盖私章的时候也是用同样方法获得这串数字12345。在他得到了这个总笔画数以后，把付款信息中的铅笔填的内容擦掉，把这个总笔画数写回去并盖上私章，后面紧跟着附上公章

逻辑较好的人会看到这里的一个问题，即：既然在付款信息一栏里已经有了前一个交易甲的总笔画数（哈希值）13524，那再把交易甲的收款信息部分填在这里再数这部分的笔画数就是不必要的，因为我已经数过了交易甲的总笔画数了，能够证明本笔交易和交易甲一一对应

对此，Talk论坛上2012年也有人质疑过
https://bitcointalk.org/index.ph ... g1123257#msg1123257
Pieter的回答是：去问中本聪（我怀疑是他主观的基于一些不成文的理由，这让他感觉更安全）
Mike的回答是：我猜这是早期版本中实现时的脚本的一种很糟糕的实现方式，后来遗留下来了

可以看到，Pieter向来就对中本聪的设计有意见，所以他现在提出完全修改比特币的架构，这个想法也是由来已久的了

最后这里是一张完整的交易单的所有16进制码，有兴趣的可以自己找找对应的那些操作码大致都在什么地方

**全部** 最佳

请发表你的真知灼见（不少于5个字）...

发表评论