### 0x01 交易隐私性

中本聪创造性的提出了比特币并且构建了一个去中心化的交易平台，从而去除了长久以来对第三方交易平台的信任依赖，但是与此同时，比特币又需要将所有的交易广播到网络上并通过所有节点达成共识来保证整个系统的安全性，也就是说所有的人都可以看到网络上所有的交易，而原始的比特币协议又并没有对交易发送者和接收者的地址作任何处理，这就导致某些细心的攻击者通过分析一个地址的交易特征并结合一些实际信息，就有可能分析出地址与实际人的对应关系，从而给使用者的隐私带来极大的隐患。基于此，门罗币首先介绍（之所以没有说定义或提出，是因为很早就有人介绍，不过是表述方式不同）了关于货币隐私的两个基本属性：

不可链接性（Unlinkability）：无法证明两个交易是发送给同一个人的，也就是无法知道交易的接收者是谁。

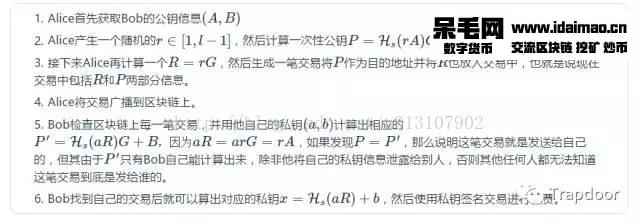
不可追踪性（Untraceability）：无法知道交易的发送者是谁。

很明显，比特币是不满足这两个属性的，交易中包含了发送者的公钥信息，而任何人都可以获取到这个信息，所以可以直接确定交易的发送者；如果两个交易的目标地址相同，那么它们肯定是发送给同一个人的，而如果接收者拥有多个地址，那么有些研究人员说通过分析每个人的交易特征，也可能确定这些地址是否属于同一个人。

而门罗币却具有以上两个属性，那么她又是怎么做到的呢？

### 0x03 Stealth Addresses (隐蔽地址)

隐蔽地址的实际思想并不复杂，就是每次发送者要发起一笔交易时，先利用接收者的公钥信息计算出一个一次性临时中间地址，然后将金额发送到这个中间地址，接收者再利用自己的公私钥信息找到那笔交易，从而进行花费，这样网络上其他的用户包括矿工等就无法确定中间地址到底属于谁的，但依然可以验证交易的有效性，而由于这个地址又是一次性的，每次都重新随机产生的，攻击者也就无法对真实的发送者接收者作任何关联。假设Alice想给Bob转一笔账，这个方法的具体实现过程如下：



从上面的流程中我们可以看出，对于Bob来说压力是非常大的，因为他需要扫描[区块链](http://www.idaimao.cn/qkl/)上的所有的交易，然后计算相应的信息进行对比才能找到发给自己的交易。门罗币为此提出了一个改进的方案，我们可以注意到，在计算P'的时候，我们只用到了(a,B)，也就是私钥的一半，而计算最终的私钥x的时候，我们必须要用到(a,b)，所以说如果某个第三方知道了a他就可以计算P'来检查交易，但却无法算出相应的私钥x从而进行花费交易，因为他不知道私钥的另一半b，基于此，Bob可以将他私钥的一半(a,B)交给一个第三方，从而授权第三方来帮忙检查区块链上所有属于Bob的交易，也就减轻了Bob的压力，但最终还是只有Bob能花费。

### 0x04 One-time Ring Signature (一次性环签名)

门罗币中引入的一个新的奇妙的技术就是环签名技术，虽然环签名在此之前就提出来了，最早的一篇文献是由D.Chaum和E.Van Heyst在1991年提出来的，但当时并不叫做环签名，而是叫群签名（Group Signature），但是这个群签名是需要依赖一个可信的第三方来参与，所以后来研究人员不断的对其改进，逐渐发展成今天稍微成熟的环签名技术，我将在下一篇文章《Ring Signature》中详细介绍环签名技术的发展以及未来可能的方向。简而言之，环签名要做的就是将签名者的公钥和另外一个公钥集合（但不知道私钥）进行混合，然后再对消息进行签名，这样对于签名验证者（任何人都可以验证）来说，无法区分混合后集合中哪一个公钥对应的是真正的签名者。

下面主要介绍一下门罗币中采用的环签名技术的整个流程。

#### 0x0401 密钥生成（GEN）

签名者首先随机选择一个私钥x，然后计算对应的公钥

同时还计算另外一个公钥

这个公钥I称之为“密钥镜像”（key image），对于每一个签名来说这个密钥镜像是唯一的，所以后面也被用来判断签名是否之前出现过。

#### 0x0402 签名（SIG）

首先签名者随机选择一个包含n个元素的公钥集合，然后和自己的公钥进行混合产生混合后的集合S，假设混合后签名者的公钥在S中的下标为s，那么他的公钥就是Ps。然后签名者再从[1，l-1]中随机选择{qi, i = 0,...,n}和{wi, i=0,...,n,i!=s}，然后计算

然后再计算一个非交互式的挑战(non-interactive challenge)，这里非交互式是相对与交互式零知识证明中的挑战而言的，在交互式中这个挑战是验证者随机选取的一个值，而因为在区块链中交易双方只能通过区块链来进行传递信息，而不能直接进行交互，所以这里选择非交互式零知识证明。而需要这个挑战的原因是避免证明者伪造证据来欺骗验证者的情况出现，详细原理请参考另一篇文章《零知识证明》。在这里，挑战的计算方式如下：

最后签名者再计算最终签名的内容，在零知识证明中称之为response：

最终的签名就是

#### 0x0403 签名验证（VER）

验证者要验证签名的有效性，首先计算

然后验证

如果等式成立，然后运行LNK来验证签名是否使用过；如果等式不成立，说明签名是非法的。

#### 0x0404 重复校验（LNK）

这要求系统必须维护一个包含所有签名的镜像的集合，然后对于每一个新的签名，通过判断它的镜像是否在集合中，来判断该签名是否之前出现过。注意在这一步之前，先要通过上一步的签名验证过程。

### 0x05 总结

门罗币通过隐蔽地址来保证不可链接性，通过环签名来保证不可追踪性，从而给用户的交易信息提供了很好的隐私性。但同时我们也可以发现，在隐蔽地址时获取incoming transaction方面给用户带来很大的压力，而且公私钥的长度也变为了原来的两倍，环签名时对于混淆公钥的选择要保证一定的随机性，签名的产生和验证过程复杂度都明显增加了，这些都是需要改进的地方。另外，交易的隐私性可能也不止就之前提到的两个属性，或许我们可以重新定义隐私，who knows?

http://www.idaimao.cn/12290.html