1. **比特币的匿名性能提供什么程度的隐私保护？**

平时谈的匿名性（anonimity）总是和隐私保护相关，即用户做的事情不想被别人知道。因为比特币系统中账户的产生不会暴露用户个人信息，用户可以产生很多对账户，然后用不同的账户做不同的事情。但这种不暴露个人信息的账户显然不是完全的匿名，可以称为假名（pseudonymity）。所以比特币系统中的匿名只是一种假的匿名，就像作家写作用笔名，网民上网交流用网名一样。

1. **和现金相比**

和现金相比，比特币的匿名性没有现金好，现金上没有任何持有者的信息（指纹之类例外），所以很多非法交易用的都是大额现金。现金的劣势就是不便于保管和运输。

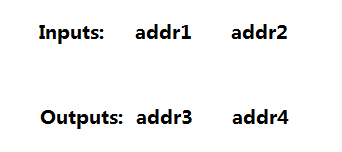
**2.** **和银行存款相比**

如果银行允许化名的话（以前国内银行不要求实名），比特币的匿名性没有银行好。因为比特币系统中所有有效的交易都写在区块链上，所有人都可以看到，而银行中的交易信息是受控制的，只有银行本身或者司法手段能获取到。但如果是现在的银行，由于开户需要身份证信息，所以匿名性比比特币要差。

1. **比特币系统中什么情况下可能破坏匿名**
2. 消费使地址账户之间产生关联

有人推崇每次收款都新创建一个比特币账户（公私钥对），这样每次使用的地址都不一样，这样做看似匿名性很高，但在比特币系统中还是常常有值得推断的地方，常常可以将不同的地址关联起来。

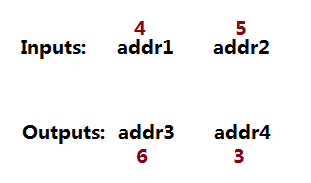
例如出现下图这样的交易：



从这个交易中，**可以推断地址1和地址2很可能是同一个人持有**，因为买东西时候很可能一个比特币账户中的钱不是正好够用，就要用到多个账户的钱。而地址3和地址4很可能有其中之一还是这个人持有，因为一个地址是卖家的账户地址，另一个地址就是**找零的地址**。

|  |
| --- |
| 这些地址可能都是比特币钱包的软件自动生成的，在找零时自动生成一个新的地址，以更好的进行隐私保护。 |

找零的地址未必在输出中的第几个位置，但可能可以分析出来，如下面是这几个输入输出中的BTC数量：



可以猜测地址4就是找零的地址，因为如果只要买价格是3个BTC的东西，不需要地址1和地址2这两个账户都动用，只动用其中一个就可以了。

现在常用的比特币钱包就那些种，只要搞清它们生成交易输入输出的方式，那么比特币系统中的大多交易匿名性也就会降低很多。

1. 地址账户和现实身份产生关联

任何让虚拟货币和现实世界发生联系的时候都可能泄露身份，其中最明显的就是资金的转入和转出。如很多人获得比特币的过程肯定不是挖矿挖出来的，而是买过来的，可以在交易所买（需要在交易所注册登记），也可以场外交易（两个人私下交易）。

很多国家有反洗钱法，如何防范用比特币洗钱的行为？只要盯住大额度的转入和转出，即大量买入比特币和大量比特币转出为法币的情况。

用比特币支付的时候也会引起隐私泄露，因为这时候也是将自己的比特币账户和自己身份关联起来了。不仅仅是向收款方泄露了自己的比特币账户，同时周围的人可以知道“这个人在这个时间用比特币消费了这家店”，然后知道知道了这家店的收款账户，再根据这个时间很容易就能在区块链上找到对应的交易记录，然后就知道这个人的比特币账户地址了。

|  |
| --- |
| 这里的一个例子是信用卡记录，即便对信用卡号码做了哈希处理，并抹掉其它个人信息，公开的信用卡记录还是可以通过这种方式在几次之内精确找到哪个人对应着哪个信用卡（卡号的哈希），所以信用卡记录是不能公开的，但比特币中的交易完全是公开的。 |

1. **如何提高匿名性？**

如果只是一个老百姓，不想让周围的亲戚同事朋友知道自己的比特币账户是哪个，有多少钱，这个相对而言是比较容易的（不要让认识自己的人看到自己用比特币支付，就可以避免前面说的类似查信用卡的方式查比特币账户）。如果是使用比特币从事非法活动，就很难保证匿名性。

比特币系统运行在应用层，其下层是P2P网络，所以可以在这两层考虑提高匿名性。

1. 网络层

当本地结点将交易发布到比特币网络上时，其它结点如果发现一直收到此账户的交易都是来自这个（或这几个）ip地址，那么就可以根据ip地址来查验身份。好在虽然区块链是新生事物，但网络层的匿名性已经有了很好的解决方案，比如**多路径转发**。

1. 应用层

前面学到破坏匿名性的一个原因就是同一个人的不同比特币账户会被关联起来，而在区块链上可以看到所有具体的交易及其来源（这个无法避免），所以可以考虑将不同人的币混起来（coin mixing）。有一些专门的网站，收取一定的费用，将所有要做coin mixing的人给的币混合起来，然后经过coin mixing再取出来再做交易。

|  |
| --- |
| 在现在的比特币环境下，没有什么信誉度很高的coin mixing服务。因为做coin mixing服务的机构的账户本身也要保持匿名，如果他们卷款跑了也很难把钱追回来。 |

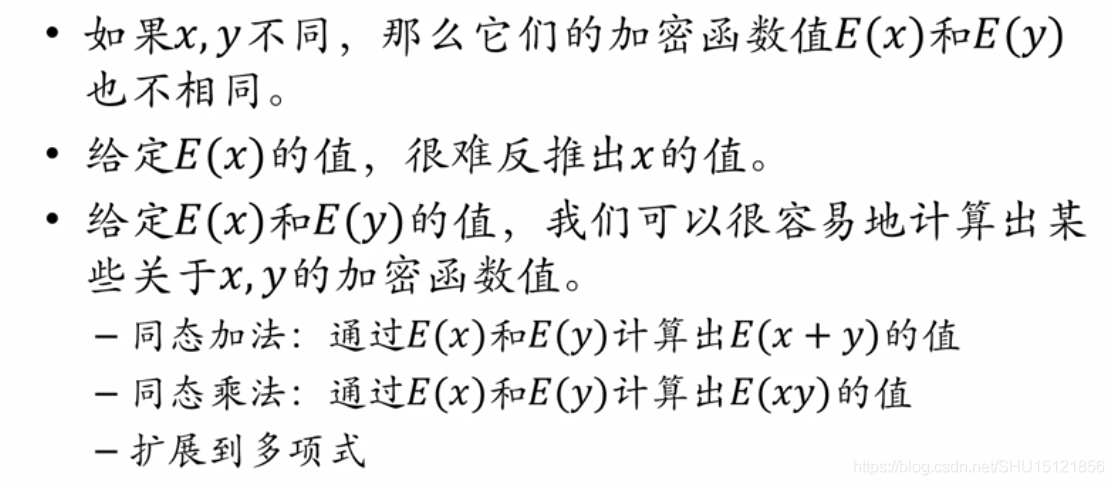
也未必需要特意去做coin mixing，有些应用本身带有coin mixing的性质，比如某些在线钱包，以及交易所。交易所天然带有coin mixing的性质，比如将比特币卖出得到法币，然后法币又买进比特币，那么买进的很可能就不是自己那条交易链上的了。但这样保持匿名性的前提是在线钱包或者交易所都不会泄露个人信息，交易所还不能泄露交易人提币和买入币的信息。

1. **零知识证明（zero-knowledge proof）**

零知识证明指一方（证明者）要向一方（验证者）证明一个陈述是正确的，而无需透露除了该陈述是正确的之外的任何信息。

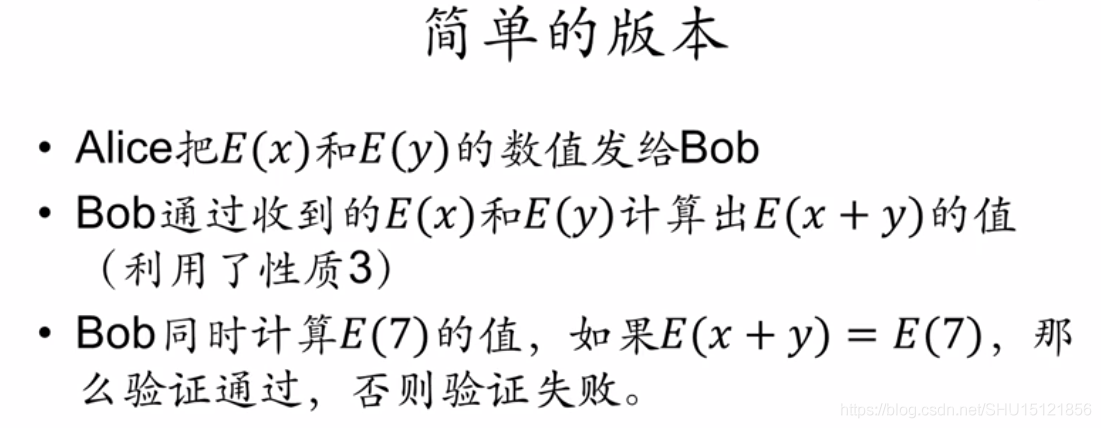
比特币系统里有一个比较有争议算不算零知识证明的内容，就是一个人要证明某个比特币账户是他的，那么只要提供一个用这个账户的私钥做的签名就可以了（这里还提供了陈述外的一些信息），验证者可以用公钥去验证。

1. **同态隐藏**



同态隐藏是零知识证明的数学基础。

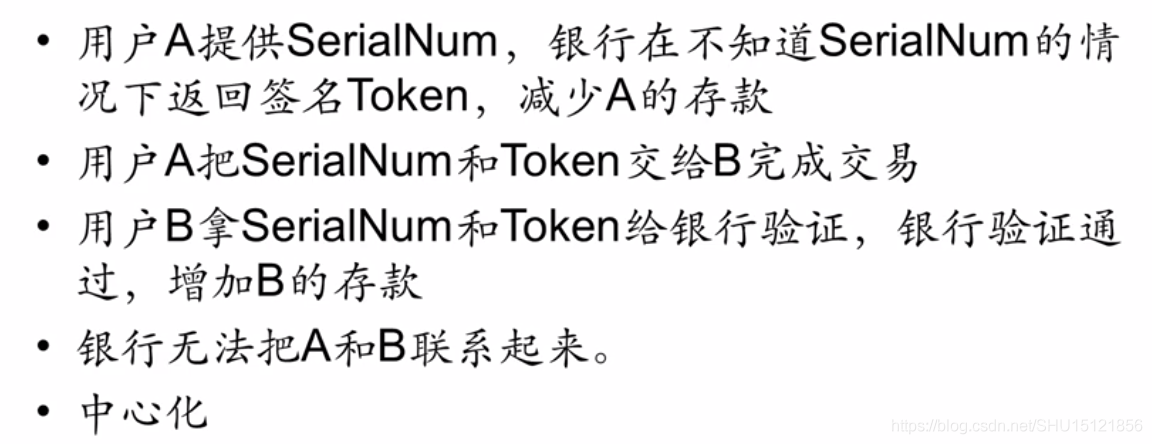
例子：



这个版本的证明方法的缺陷是Bob可以用蛮力计算的方法试出原来的x和y是多少。在更复杂的解法中，需要Alice对x和y做一些随机化处理，但保证x和y加起来的值是不变的。

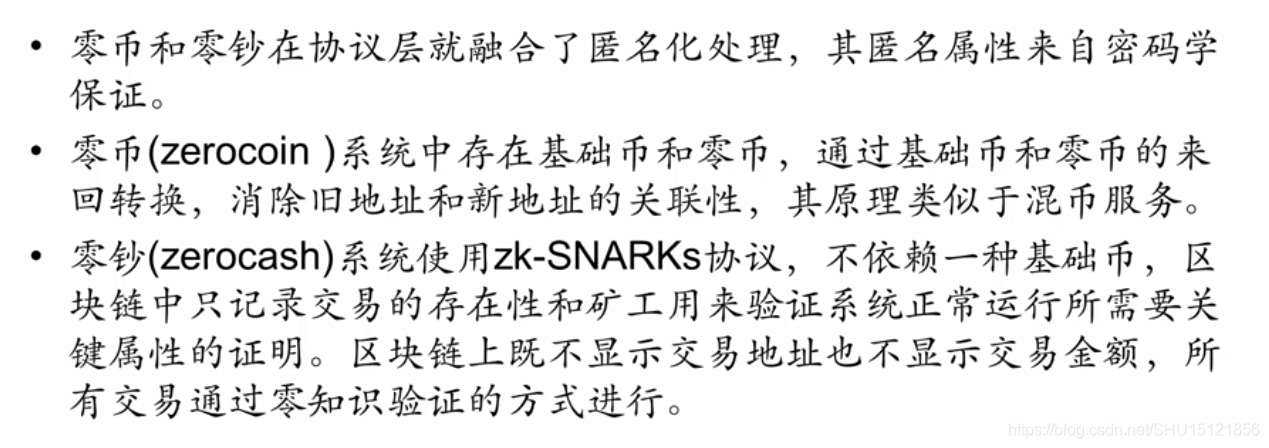
1. **盲签**

在前面学习共识协议里，中心化的方案中央行要维护一个数据库，记录签发的货币在哪个用户手里，但这样央行就知道了用户之间的货币流通，不利于匿名性。盲签可以解决这个问题。



1. **零币和零钞**

比特币在一定程度上提供了匿名性，但无法完全消除关联性。零币和零钞就是为此问题设计的加密货币，运用密码学原理保证匿名性。



这里基础币是既有的一种币，比如比特币，然后将其变成花不出去的状态换取零币。在花零币的时候，只要通过零知识证明证明花的是系统中的多少币，而不需要说明花的是哪些币。

零币和零钞还不是很流行，原因是很多方面的：

* 为了匿名性，损失了一些性能
* 对初始化有比较严格的要求，初始化使用的随机源要能很好的销毁掉，否则会有安全漏洞
* 需要强匿名性的用户不多（大多不做非法洗钱之类的事情）
* 与现实世界发生交互时，仍然会破坏匿名性

总结

比特币的匿名性并不好，保证用户隐私难度很大，本质原因是区块链上的交易是完全公开的，并且是不可篡改的。这种不可篡改性看似很美好，其实对隐私保护是灾难性的，因为一旦某个交易泄露了隐私，这个交易却永久的在区块链上无法抹除。