

比特币科普及其未来三种结局

詹臻臻 zhanzhenzhen@hotmail.com i@zhanzhenzhen.com

扫盲

到底什么叫比特币啊？我觉得网上缺少能使非专业人士迅速理解比特币的文章，于是自作聪明写了前两章“科普”（只用到了小学里面的数学知识），写得不好的地方还请多多包涵。

我们通常上网，如果网站能保存用户资料，那一定是有账户的。但在比特币的世界中，压根就没有所谓“个人账户”的概念，而是针对每笔钱，有着对应的**2把钥匙和1个地址**：

- **私钥**。谁知道了私钥，谁就能控制这笔钱。因此通常都是这笔钱的主人才知道（千万不可泄漏）。
- **公钥**。全世界都将知道。只在程序内部使用。
- **地址**。性质很像公钥，但比公钥短。收钱时你就把地址告诉别人。

为什么要用到“私钥”和“公钥”啊？安全吗？其实这都和**密码**有关，叫做“**非对称密钥**”，下面让我们来讨论一下非对称密钥（下一章对于理解比特币非常重要，请耐心等待）。

非对称密钥、哈希与交易

你用过WinRAR等工具加密文件吗？其实加密文件，就是把看得懂的字符，用你输入的密码进行某种数学运算，从而变成乱码。而解密呢，就是把乱码还原（用你输入的相同密码进行反运算）。这类加密和解密使用相同密码的方法叫做“对称密钥”。

那有没有加密和解密使用不同密码的呢？也有！这就是“**非对称密钥**”，两个密码分别称做“私钥”和“公钥”，它们并非互相独立，而是通过某种关系一一对应，并具有如下两个魔力：

- 私钥加密的信息，只有公钥才能解密；公钥加密的信息，只有私钥才能解密。
- 从私钥算出公钥很容易，但反过来，从公钥算出私钥极其困难。

这有啥用啊？我们一步步来，先说下为什么从公钥算出私钥是极其困难的：

有一种算法，以两个质数（素数）的集合为私钥，以它们的乘积为公钥。其安全性如何？

我们取{29,53}作为私钥，取它们的积1537作为公钥。如你知道私钥，那必然能算出公钥，只要相乘就可以了；如你知道公钥，也必然能算出私钥，因为任何合数分解质因数都是唯一的，

但要慢得多，因为要不断地试错，从2,3,5开始除，试到29才整除。实际应用中，私钥取两个很大的质数，那么就认为不可能从公钥算出私钥了，例如：

123018668453011775513049495838496272077285356959533479219732245215172
64005072636575187452021997864693899564749427740638459251925573263034
537315482685079170261221429134616704292143116022212404792747377940806
65351419597459856902143413 =
334780716989568987860441698482126908177047949837137685689124313889828
83793878002287614711652531743087737814467999489 ×
36746043666799590428244633799627952632279158164343087642676032283815
739666511279233373417143396810270092798736308917

一台电脑要运算几百年才能分解这个数字，而比特币的私钥比这更安全，因为使用的是更高级的方法（基于椭圆曲线的离散对数，能以更小的密钥长度提供更好的安全性，数学原理十分复杂，这里不作讨论）。

比特币“某笔钱”的私钥、公钥和地址是类似这样的：

程序随机生成一个私钥，例如

asdfghjkqwertyuiopzxcvbnm123456789QWERTYUPASDFGHJKZX，储存在你的硬盘里，不外泄。

根据该私钥算出公钥，例如

PUYTREWQLKJHGFDSAMNBVCXZ987654321poiuytrewqkjhgfdsamnbvcxzQAZWSXEDCRFV，以后会上传到全网。

根据该公钥算出地址，例如zaq1XSW2cde3VFR4bgt5NHY6mju7K8Lo9p。地址是怎么算出来的，我们稍后再说。

当你要发送一笔钱给某人时，你输入金额和对方的地址，程序会为你创建一条消息，如“我发送100枚比特币至地址4rf...ki8”。然后，关键的是，程序对这条消息用私钥加密，这个过程就是著名的“**数字签名**”。**签名不能保证消息不被人看到**（因为任何人都有公钥可以解密），**但能保证消息不被伪造**（因为别人不知道你的私钥，如果有坏人用他自己的私钥签了条消息，然后发到网上说是你签的，那大家一定无法用你的公钥来解密，验证一定是失败的，这里公钥能否成功解密就是用来验证签名是不是伪造的）。

把经过签名的消息，附上公钥，组合起来，就构成了一笔完整的交易，然后可以把该交易发布到全网。

下面介绍另一种魔力，叫做“**哈希**”，地址就是“**哈希**”而成的。

哈希又称指纹、摘要、杂凑，它顾名思义，使用“小特征”来标识“大东西”。正如每个人有不同的指纹，每个文件、每段文字，只要内容稍有不同，就有不同的哈希值。以MD5哈希算法

为例，任你再大的文件，大到100GB，都可以计算出它的32字符哈希值。

例子：

Lorem ipsum dolor sit amet, consectetur adipisicing elit, sed do eiusmod tempor incididunt ut labore et dolore magna aliqua. Ut enim ad minim veniam, quis nostrud exercitation ullamco laboris nisi ut aliquip ex ea commodo consequat.

MD5哈希值：1af9a54677a2889a20a16218ba5be4f4

Lorem ipsum dolor sit amet, consectetur adipisicing elit, sed do eiusmod tempor incididunt ut labore et dolore magna aliqua. Ut enim ad minim veniam, quis nostrud exercitation ullamco laboris nisi ut aliquip ex ea commodo donsequat.

MD5哈希值：0dd03063ca945d0190b8920315b53cea

这两段文字几乎完全相同，除了最后一个单词的c改为了d，但是哈希值完全不同，哈希算法厉害吧？那如果另一段文字也有相同的哈希值，怎办？这理论上可能，但你采用“暴力破解”的话，得用n多含不同字符的文字试验，试300万亿亿亿亿（ 2^{128} ）次左右才能找到，所以实际上不可能，这比两个人指纹相同的概率更小。哈希的用途很广泛。如你下载一文件，你事先知道它的哈希值应该是多少，那么当下载完毕，可以给文件算一下哈希值，如相同，则证明文件没有被篡改（没感染病毒），否则该文件就比较危险。现在一般大公司出品的安装文件在“属性”窗口里都能看到“数字签名”，它签的就是文件的哈希值，并不需要签整个文件，这样就能保证文件在传输途中没有被篡改。

回头看前面的例子，用私钥加密消息“我发送...至地址...”，说得并不确切。实际上为了节省成本（非对称密钥的加密解密极其消耗CPU，而消息可能非常庞大），签名都是加密消息的哈希值，而不是加密消息本身。所以一笔完整的交易是：消息、（消息的哈希值的）签名、公钥。

为什么既有公钥，又有地址？这是因为公钥太长了，所以把公钥“哈希”一下变成34字符的地址，收付款时更直观，而公钥就只在程序内部使用了。但地址也不能太短，否则这个哈希算法容易被破解，出现两笔钱的地址相同。

私钥→公钥→地址，推算过程是单向的，无法逆向推算。无法从公钥推算私钥前面已说明；由于哈希算法会损失信息，所以也无法从地址推算公钥。

由此可知，比特币是“只认私钥不认人”的，严格说来没有所谓“拥有”的概念，或者说，控制即是拥有。你也可以“拥有”多笔钱，因为你可以创建多个私钥。私钥创建好后，该笔钱即具有初始余额0，当有人付款到它的地址时，余额就会增加。

如果你看到这里看懂了，那你就基本了解了比特币的运作机理，而且我敢说你已经基本了解了貌似很高深的密码学。因为正是对称密钥、非对称密钥、哈希，这三者构成了现代密码学的一切。（至于反过来，公钥加密、私钥解密的体系，虽然比特币用不到，不过在其他领域是极有

用的，涉及到：如何传递密码本身？读者有兴趣的话可以思考一下。）

注：比特币协议中真正的“交易”记录比这个更复杂，但基本原理是一样的。

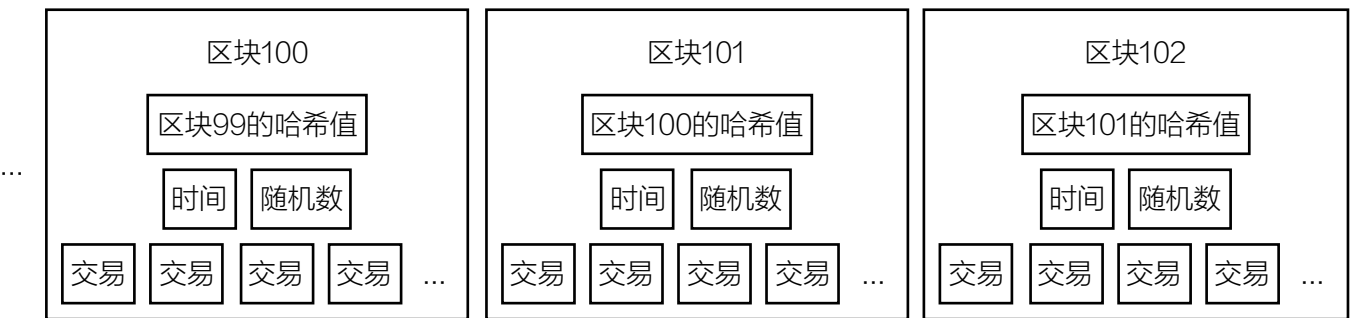
比特币很像黄金，因为它的**总量限定在2100万枚**，不会超发。

进阶：时间问题及其解决方式

这一章如果看不懂没关系，观其结论即可。比特币发明者**中本聪**的原始论文比较详细，本文篇幅所限只能压缩。

现在有一个问题，就是无法给交易注上时间。如果有一台服务器，那简单，只要使用服务器上的时间就行了。但比特币没有服务器，世界上现存很多“时间服务器”，也不能为比特币所用，因为比特币的精神就是不信任任何机构发布的数据，甚至连它自己的官方网站的数据它也不信！那么用交易者自己电脑上的时间行不行呢？更不行，因为伪造自己电脑的时间太容易了。那可如何是好？中本聪想出了“**块链**”和“**挖矿**”来尝试解决这个问题。

挖矿软件运行时，程序会接收全网所有最新（约10分钟内）的交易，把它们保存在一个临时“**区块**”中。程序向区块中加入时间和一个**随机数**，计算区块的哈希值，如果哈希值满足一定条件（例如前8位都是0），则成功，否则就改变该随机数继续试。例如第一次哈希值是3f5...（16进制），那么再试第二次，直到某次哈希值为00000000ae9...。（为鼓励人们贡献自己电脑的算力，算出的人可以得到25枚比特币的奖励，所以这个过程被形象地称为“挖矿”。挖矿的几十万台电脑全力运算约10分钟才能偶尔成功1次，难度可想而知，所以一台电脑成功挖到矿的概率和中彩票差不多。）然后把该哈希值发布到全网，网络验证了其中每笔交易都有效且之前从未出现过以后，该区块就被正式加入进块链中来。下图是一个块链的例子：



你问比特币在时间问题上信什么？**信最长的块链**。通俗点说，就是信CPU算力。如果坏人想要修改一个区块，例如删除一些交易，或修改下时间，那他就必须重新计算生成这个区块以及它之后的所有区块（否则哈希值对应不起来），以使他自己的块链达到最长，这样才能被全网所接受，但这谈何容易！所以越老的交易，越不容易被删；越新的交易，越容易被删。如果全世界大多数挖矿的CPU为不法分子所掌控，那么比特币全网就可能陷入瘫痪，因为所有区块都能被改写，所有交易都能被删除。如果全世界总共1000个CPU挖矿，坏人掌握了其中100个（1/10），那么他们虽无法使全网瘫痪，但有相当的破坏能力，例如有约1/10的把握能破坏最后的区块，有约1/100的把握能破坏最后第二个区块，依此类推。

这就是为什么比特币官方建议大额收款要等待6个确认。1个确认代表1个块的生成。只等1个确认，只需10分钟，但此交易被删的可能性比较大。如果你花60分钟等6个块生成后，发现交易还在，那被删的可能性就很小了。

注：交易可能被删，但无法被篡改，因为签名是无法伪造的。

（问：那不还是要相信某台挖矿电脑上的时间吗？答：是的，但由于诚实的CPU一般占绝大多数，故时间被“恶搞”的几率较小，而且比特币官方客户端中作了限制，例如区块的时间不得早于之前11个区块的时间的中位数，也不得晚于某值，等等。）

被动收款与主动收款

下面我们花几章来探讨下比特币究竟有哪些不足之处。

如果有人突然打你电话，说他刚付给你一笔钱，你可不要以为只需等待6个确认就保险了，事实上可能要等待12-18个确认才够安全。这个问题在中本聪的论文里有阐述：

The receiver generates a new key pair and gives the public key to the sender shortly before signing. This prevents the sender from preparing a chain of blocks ahead of time by working on it continuously until he is lucky enough to get far enough ahead, then executing the transaction at that moment.

作者建议要尽可能晚告诉付款人你的地址，并建议每次收款都用新地址。因为付款人如果事先知道你的地址，就可能连续花费数个月去计算，等到某天某时刻他运气好得让他自己的块链领先了6个块，立即在主块链上生成一个交易，打你电话说他付款了。这样，虽然你等了6个确认，但他还是可以在最后把自己的块链覆盖上去，从而删除该付款。

我把这样的收款叫做“被动收款”。对付这类人的办法有三个。第一个就是中本聪论文里面的方法，但这样太麻烦；第二个是“主动收款”，即你令付款人必须在指定时间付款；第三个是等待更多的确认。显然，这三个办法都称不上完美。

真的可以消灭“信赖”吗

比特币名义上是不依赖任何机构的。但其实，不管你是把私钥写纸上塞进保险箱，或者写入U盘再把U盘放进保险箱，或者保存在电脑里，你都需要信赖一些事物。首先，如果你已经结婚，那你需要信赖你的伴侣和你一条心，不会取走你的私钥。如果你保存在电脑里，那你需要信赖微软或苹果或别的什么厂商，不会盗取你的私钥。如果你有10000枚比特币，也许你会选择把存放私钥的U盘放在某大银行的保管箱里，那你同样需要信赖这家银行不会盗取你的私钥。你会发现像比特币信徒所宣称的可以完全消灭“信赖”和“信用”是不可能的事。既然如此，为什么还要去消灭信赖呢？

比特币这种“只认私钥不认人”的特性会产生严重的安全问题，即万一你的私钥被盗取，钱就

成了别人的了。我认为这可能会催生一种第三方比特币托管的服务。这种服务中，第三方公司面向用户采用个人账户的概念，提供钱款安全的保障，但公司内部使用私钥、公钥、地址和比特币网络进行通信（用户并不知道私钥），如私钥被盗，损失由公司承担。在这个模式中，可见你仍需信赖这家看起来像银行的公司。

这种通过第三方公司作为中介来缓冲的方式，也能够部分解决每次交易需要10-60分钟的大难题。当你需要快速花一笔小钱，公司看到你账户的余额还很多，会以公司的信用向商户承诺：“如果交易被人恶意取消的话我们会继续付款直到成功”，同时冻结这笔钱，保证不被你挪作他用。当然这种方式只适合于小额支付。

反正我就一个人生活

读到这儿，有的比特币信徒可能会耍赖：“反正我就一个人生活，我的CPU是自己焊的，操作系统是自己写的，这总可以不靠别人了吧？”好，就算你能避免所有的信赖，你总不能不信赖比特币协议和官方客户端的开发人员吧？我也是个开源（尤其是底层开源）的爱好者，但我认为，开放源代码虽然从长期来看可以使程序更健壮和安全，但从短期来看并不能避免突然出现恶意代码。须知，开发人员只占比特币爱好者的少数，如何防他们集体叛变？事实上，在开发人员中也不可能绝对民主，只要权限最大的几个人突然叛变，就够呛了。我相信社区有自我调节能力，但短期内仍会引发损失。这种损失可不只是删除最近交易、瘫痪网络之类的小儿科，恶意代码甚至会使你电脑中毒，从而盗取私钥，伪造签名和交易。所以，你还是要像相信别的公司、组织一样，去相信他们。

哈希碰撞与量子计算机

如果哈希算法SHA256被找到漏洞，那么将可以轻易生成两个具有相同哈希值的不同消息，这被称为“碰撞”。不过这是可以补救的，中本聪在2010年写到，可以升级比特币协议，使之只接受采用更强哈希算法的区块，然后计算所有旧区块合起来的一个哈希值（用新算法），将该值写入比特币协议中，这样就能保证旧区块的安全。由于有这个补救方法，且SHA256被攻破的可能性较小，所以无需特别担心。（我国的王小云教授在2005年找出了MD5、SHA0、SHA1的漏洞而震撼了密码学界，比特币是2008年诞生的，中本聪选择了更强的SHA256。）

对比特币而言真正的问题是量子计算机。量子计算机在不远的将来（也许是10年内）就将诞生，它已经被证明可以破解当今最流行的两种非对称密钥算法，即前面提到的基于分解质因数的RSA算法和比特币使用的基于椭圆曲线的ECC算法。在一开始的例子中，如此大的合数，一台普通电脑要运算几百年才能分解，但量子计算机使用Shor算法（一种量子算法）可能只需不到1秒就可以分解了。即：**量子计算机可以从公钥算出私钥**。为此，比特币将不得不新增一种“抗量子”的非对称密钥算法，例如“格密码”。

但是这种方法，是强令用户时刻关心比特币新闻。某天，比特币官方可能会宣告：“1年以后量子计算机就将诞生，届时大家的私钥都将不安全。我们现在推出采用新算法的私钥，希望大

家创建新私钥，把老私钥的钱都转移到新私钥。如1年之后还未转移，对于您的损失我们概不负责。”有这个巨大的缺陷，怎么说服今天的人们把钱存进来？这会让那些抱有“一个私钥存在一个安全的地方就能保有一辈子”想法的人失望。如果你现在认为你的私钥是绝对安全的，再也不关心比特币的新闻了，你恐怕到时候也不会想到去更改私钥，私钥一旦被人算出，那你的钱就全完蛋了，你甚至无法把他们告上法庭，因为没有任何证据证明这私钥就是你的，比特币可没有账户。

未来场景

我觉得，中本聪在发明比特币时肯定是希望集全世界PC之力，大家分散地用CPU挖矿的，但没想到后来发展到用显卡挖矿，现在更是到了哈希专用芯片挖矿的地步（这种机器卖到了几十万RMB一台，速度是普通电脑的数千倍），以至于现在官方客户端都取消了挖矿功能。这将导致算力趋向于被寡头所把持，因为老百姓不可能花几十万买这样一台矿机。那你又得信任这些寡头。比特币官方也许会说：“没人会那么傻，他们有那么强大的算力，不会诚实地挖矿赚钱啊，干嘛要破坏？”但想不想破坏和有没有能力破坏是两码事，我们为什么要让他们有能力破坏呢？何况，在钱的激励下去破坏也是有可能的，让我们设想某“未来场景”：

M₁、M₂、M₃是全球最大3家挖矿公司，算力总和达到全世界的60%。B是商户，P是个坏人。P想获得B的某款价格为฿1000的商品，于是他向这3家寡头各支付฿200好处费，待P向B付款฿1000后，B等了超过6个确认，认为万无一失了，于是发货。这时“三巨头”联合起来用计算优势删除了这个交易，导致฿1000又退回给了P。这样，三巨头虽然没把算力用在挖矿上而损失了部分比特币，但它们通过收黑心钱赚到了更多（฿600），而商户损失了฿1000。事实上，这三巨头已不是“挖矿公司”，而是已成为“删交易公司”，平时就联合起来帮给钱者删，而各自挖矿只是副业而已。

（฿是比特币的货币符号。以上场景纯属虚构，但并非不可能出现。）

趋势

当今世界的趋势是节能，经验告诉我，浪费电的产品不会有前途。挖矿对于CPU算力有不可思议的消耗，这种消耗体现了比特币的核心思想，所以永远都不会减少或消失。等到2140年矿都挖完了，也必须维持住这种电力消耗，以保证安全，不在跟坏人的块链长度竞赛中败北。但没有激励了，谁会每天24小时耗100%CPU去参与这种运算？于是它会推出交易费，交易费分给参与者。由于这种电力消耗远远多于采用服务器方案的电力消耗，所以交易费必然会远大于其他电子货币。所以比特币就算能坚挺到2140年，以后也将不具竞争力。

在2140年全部2100万枚比特币被挖出来后，比特币会持续地通货紧缩，因为人们会不断死去，会有部分人去世前没把私钥告诉家人。这样，比特币总量会越来越少。公平地说，这并不是比特币的弱点，因为它可以无限分割。现在比特币最小单位是0.00000001，若哪天全人类只有1枚比特币了，那么最小单位可以设为0.0000000000000001，再修改下客户端就OK了。

但从Web发展趋势来看，我认为需要安装软件的玩意儿都会被淘汰，未来所有事情都将可以用浏览器来解决。浏览器未来会支持纯P2P吗？似乎不可能。浏览器现在最多也只能用来访问比特币相关公司的网站。

重回信用体系

算法能无缝升级正是服务器的好处。当量子计算机将要问世，或某算法变得脆弱时，管理员可以升级算法，用户不需关心或改动任何东西。所以，基于信用的体系，天生就具有可改进、可升级的能力，即使某个算法未来被破解，也没什么关系。

基于信用的体系，还能从根本上解决交易被破坏的问题。不存在什么等待10分钟的被删率是多少啦，等待60分钟的被删率是多少啦等等，而是每个交易都可以瞬间完成，且绝不会被破坏，只要服务器的拥有者可信的话。

基于信用的体系，还能使用户更安全，即使密码被盗，也可以用绑定的手机恢复。服务器还能轻而易举地给交易注上时间，而不用像比特币那样复杂、低精度（误差约10分钟）且不完全可靠。

其实这就是一个可靠度的大小的问题。如果某国际组织（例如联合国）发行了一种依靠服务器的电子货币，它的可靠度可能是99.99%。那比特币呢？可能很高，也可能只有90%或更小。既然比特币也到不了100%，那我们（特别是极客）为什么还要痴迷于它不放呢？

结论：三种结局

第一种，比特币**大一统**。当前世界货币总量（供应量M2）约为100万亿美元。这样，每枚比特币值**500万美元**，可能性5%。

第二种，比特币**取代黄金**，成为首选的保值产品。2010年地上黄金总存量16.6万吨，总市值7万亿美元。假设用于首饰和用于投资的黄金各占一半，那么用于投资的黄金为3.5万亿美元。这样，每枚比特币值**17万美元**，可能性5%。黄金基本上是一种总量稳定的东西，当然理论上不能排除今后通货膨胀的可能，例如在某颗行星上或太阳系外发现了10倍于地球储量的金矿，那可能黄金就会被取代。

第三种，比特币**被淘汰**，价值归零，可能性90%。但是，我不认为现有的各国法定货币是终极货币。人类可以设计一个世界的、完全无纸的、至少可以代替黄金的电子货币，中本聪的一些思路我们可以借鉴，但不能没有服务器（笔者倒有个初步方案，或许可以两全其美，这里就不讨论了）。沿着比特币的方向，很遗憾，即使没有政治上的阻力，这也是一条歧路。

（欢迎转载，转载时请注明作者）

签名: Zhenzhen Zhan

Zhenzhen Zhan (Mar 15, 2014)

电子邮件: zhanzhenzhen@hotmail.com

比特币科普及其未来三种结局

EchoSign Document History

March 15, 2014

比特币科普及其未来三种结局

上传者: zhanchenzhen@hotmail.com | zhanchenzhen.com

扫盲

到底什么是比特币呢？我发现网上缺少能使非专业人士迅速理解比特币的文章，于是自作聪明写了这篇“科普”（只用到小学程度的数学知识），写得不对的地方还请大家包涵。

我们通常上网，如果网站能保存用户资料，那一定是服务器端的。但在比特币的世界中，这根本就不叫“个人用户”的概念，而是针对网络地址。有像比特币这样的虚拟货币和数字货币。

- 私钥，谁知道了私钥，谁就能控制这笔钱。因此通常都是这笔钱的主人知道（千万不可泄露）。
- 公钥，全世界都知道，只在程序内部使用。
- 地址，性质像公钥，但比公钥短。收钱时你就要把地址告诉别人。

为什么需要“私钥”和“公钥”呢？安全问题！其实这和密码学有关，叫做“非对称加密”。下面我们再来讨论一下非对称加密（下一篇对于理解比特币非常重要，请耐心读完）。

非对称加密、哈希与交易

你用过WinRAR的加密文件吗？其实加密文件，就是把要传输的字符串，用你输入的密码进行某种数学运算，从而变成乱码。而解密呢，就是用你输入的相同密码进行反运算。

这类加密和解密使用相同密码的方法叫做“对称加密”。

那有没有加密和解密使用不同密码的呢？也有！这就是“非对称加密”，两个密码分别叫做“私钥”和“公钥”，它们并非互相独立，而是通过某种关系一一对应，并具有如下两个能力：

- 私钥加密的数据，只有公钥才能解密；公钥加密的数据，只有私钥才能解密。
- 从私钥推出公钥很容易，但反过来，从公钥推出私钥极其困难。


这有啥用呢？我们一步步来，先说下为什么从公钥推出私钥是极其困难的：

有一种算法，以两个质数（素数）的乘积为公钥，以它们之和为私钥，其安全性如何？我们举255位作为私钥，取它们的积157作为公钥，如何？如果你能算出私钥，那必然能算出公钥，只要你有足够的时间了；如果你能算出公钥，也必然能算出私钥，因为任何两个质数乘积都是唯一的。

“比特币科普及其未来三种结局” History

 Document created by Zhenzhen Zhan (zhanchenzhen@hotmail.com)

March 15, 2014 - 6:58 PM GMT+8 - IP address: 61.171.191.178

 Document signed by Zhenzhen Zhan (zhanchenzhen@hotmail.com)

Signature Date: March 15, 2014 - 7:00 PM GMT+8 - Time Source: server - IP address: 61.171.191.178

 Signed document emailed to Zhenzhen Zhan (zhanchenzhen@hotmail.com) and 26268224@qq.com

March 15, 2014 - 7:00 PM GMT+8