大家好，今天来为大家解答比特币中的量子这个问题的一些问题点，包括比特币量子也一样很多人还不知道，因此呢，今天就来为大家分析分析，现在让我们一起来看看吧！如果解决了您的问题，还望您关注下本站哦，谢谢~

本文目录

比特币的数学原理是什么？

比特币的数学原理加密算法一共有两类：非对称加密算法（椭圆曲线加密算法）和哈希算法（SHA256，RIMPED160算法）。

椭圆曲线加密算法

试想有一种乘法，可以在已知a,b的情况下计算出c=a*b，但已知c,a不能计算出b。

我们可以利用这种乘法进行加密解密。

设明文m，密文g1,g2。

用公钥a,c=a*b,r（随机数）加密：

g1=m+r*c

g2=r*a

用私钥a,b解密：m=g1-b*g2

证明：

g1-b*g2

=m+r*c-b*r*a

=m+r*c-r*c

=m

我们还可以利用这种乘法进行签名认证。

设原文m，签名g1,g2。

用私钥a,b,r（随机数）签名：

x=r*a

g1=SHA(m,x)

g2=r-g1*b

用公钥验证：

g2*a+g1*c

=(r-g1*b)*a+g1*c

=r*a-g1*b*a+g1*c

=r*a-g1*c+g1*c

=r*a

=x

计算SHA(m,x)是否和g1相等。

这就是加密解密层面上的椭圆曲线加密算法。

比特币私钥(privatekey)，公钥(publickey)，公钥哈希值(pubkeyhash)，比特币地址(address)

公钥和私钥由椭圆曲线加密算法生成，私钥可推出公钥而反之不能。

有了私钥，你就可以对文本签名。别人拿了你的公钥就可以根据签名认证你是否拥有私钥。这就是证明你拥有存款的办法。

为了安全起见，公钥应该隐藏起来。所以对公钥进行哈希加密，生成公钥哈希值然后计算哈希值的比特币地址：

公钥哈希值=RIMPED160(SHA256(公钥))

比特币地址=*1*+Base58(0+公钥哈希值+校验码)

校验码=前四字节(SHA256(SHA256(0+公钥哈希值)))

可以看出，地址和公钥哈希值是等价的（可以互推）但公钥哈希值只能由公钥算出（不能逆推）。

验证的时候需要提供签名和公钥，算出公钥哈希值并和比特币支出脚本的公钥哈希值对比，最后再验证签名。这样就保证了公钥不会出现在支出脚本里。

（收入单提供签名，支出单提供公钥，或者收入单提供签名和公钥，支出单提供公钥哈希值，这两种验证办法是比特币的标准脚本）

哈希(Hash)算法

哈希算法（又称散列算法）不是加密解密算法，因为其加密的过程是不可逆的（你只能加密不能解密），也没有所谓的公钥私钥的概念。

哈希算法原理是将一段信息转换成一个固定长度的字符串。这个串字符串有两个特点：

1、如果某两段信息是相同的，那么字符串也是相同的。

2、即使两段信息十分相似，但只要是不同的，那么字符串将会十分杂乱随机并且两个字符串之间完全没有关联。

信息可以是一串数字，一个文件，一本书。。。。。。只要能编码成一串数字即可。

显然，信息有无数多种而字符串的种类是有限的（因为是固定长度），所以这种加密是不可逆的。

哈希算法的用途

1、验证两段信息是否相同。

A使用QQ给B传了一个文件，这个文件会在QQ的服务器上保存下来。如果C也传了这个文件给D，QQ会对比这个文件的哈希值和A传给B的文件的哈希值是否相同，如果相同则说明是同一个文件，C就不需要再一次上传文件给服务器。这就是所谓的秒传。

一个压缩包在传输的时候可能会有损坏。在压缩之前计算原文件的哈希值并放入压缩包中，待解压后再次计算解压文件的哈希值。对比压缩包中的哈希值则可以知道文件是否损坏。BT和迅雷下载中所谓的哈希验证也是同一道理。

2、验证某人是否信息持有者。

在一个论坛注册帐号，如果论坛把密码保存起来，因为无论坛多么安全都可能会被破解，所以密码总会有泄漏的可能性。

如果不保存密码而保存密码的哈希加密值。当你下次登陆论坛的时候，将你输入的密码的哈希值和你注册时密码的哈希值比对，如果相同则可以证明你就是密码持有者了。这样既保证了密码泄露的可能，又保证了验证持有者的功能。

哈希算法的破解

假如论坛被破解了，黑客获得了哈希值，但黑客只有哈希值依旧是不能登陆论坛的，他得算出用户的密码。

他可以随机产生密码一个一个试，如果算出的哈希值正好和这个哈希值相同，则说明这个密码可用。这就是所谓的猜密码。

显然，密码长度越长，密码越复杂，猜到的可能性就越低。如果有一种办法能增加这种猜到可能性，使其大到能够容忍的范围，则该哈希算法被破解了。

例如原本猜中的概率是1/10000000000000，现在增加到了1/1000。如果每猜一个密码需要1秒，按照之前的概率猜知道太阳毁灭都可能没猜中，但后者只需要1小时就足够了。

另外，由于信息的种类是无限的，所以你猜中的密码未必就是原先的密码，它们可能是碰巧哈希值相同而已，这就是所谓的碰撞。

如同增加猜中概率一样，如果能增加碰撞的概率，那么同样可以轻易登陆论坛（因为论坛也不知道原本的密码是什么，所以猜的密码和原密码不同也没关系，只要哈希值相同即可）。

一旦碰撞容易轻易产生，那么哈希算法就被破解了。前几年闹得沸沸扬扬的哈希算法破解就是这么回事，数学家通过一定办法增加了碰撞的概率。

哈希算法的大致加密流程

1、对原文进行补充和分割处理（一般分给为多个512位的文本，并进一步分割为16个32位的整数）。

2、初始化哈希值（一般分割为多个32位整数，例如SHA256就是256位的哈希值分解成8个32位整数）。

3、对哈希值进行计算（依赖于不同算法进行不同轮数的计算，每个512位文本都要经过这些轮数的计算）。

经过这样处理以后，哈希值就显得十分杂乱随机了。

非对称加密算法

非对称加密算法是世界上最重要的加密解密算法。所谓非对称，是指加密和解密用到的公钥和私钥是不同的。非对称加密算法依赖于求解一数学问题困难而验证一数学问题简单。

RSA算法

著名的RSA加密算法就是利用了对一个大整数进行因数分解困难，验证因子组成某个大整数容易的原理而编写的。

具体说，比如求143的因子，你可能需要进行11次除法才能得到143=11*13的结果。但是要验证11*13=143，则只需要一次乘法就够了。

如要破解RSA，只需要能够快速分解大整数即可，显然这是破解RSA最简单最快速的办法。但要分解大整数是极不容易的（数学上叫做NP-Hard问题），这也就是RSA能保证其不能被破解的原因。

反之，如果人类某天找到了快速分解大整数的办法（例如利用量子计算机进行计算

），则RSA算法就立即被破解了。

RSA算法的大致原理

生成公钥和私钥：

1、生成一对大质数p,q，求出n=p*q和f=(p-1)*(q-1)。

2、生成一个随机数e，满足e<f且e,f互质。

3、求出e关于f的模逆d，即求出e*d=1modf。

设明文为m，密文为g。

用公钥n,e加密：m^e=gmodn

用私钥n,d解密：g^d=mmodn

证明解密后的明文就是原先的明文：

根据加密解密规则，将g=m^emodn代入g^d=mmodn后，发现只要证明m^(e*d)=mmodn即可（同余运算的原理）。

由于e*d=1modf，所以只需证明m^(f+1)=mmodn即可。根据欧拉定理，f是欧拉函数所以得证。（具体的数学原理这里不再赘述）

显然，如果知道了f，就可以根据公钥n,e计算出d破解明文。要知道f，必须得知道p和q。要知道p和q，必须将n分解。所以RSA的破解依赖于整数分解。

比特币的价格是和底层技术无关吗？

价格和交易量与投资有关。交易量与交易的效率有关。交易/效率与平台技术和规则有关。在没有监管时，平台规则和技术就是交易/效率的支撑。也就是间接与交易价格相关。重要前提是正常交易，也即平台/平台操作者都是干净的。

如果军方实现了量子计算机就能破解比特币私钥以卖币补充军费吗？

如果比特币系统所采用的非对称密码不进行相应改进，量子计算机出现之后，确有可能破解现有的非对称密码系统。

破解现有非对称密码系统之后，破解者确实有可能破解比特币系统的私钥，获得更多比特币。但这与是否是军方没有必然联系，这是全球范围内所有主权国家之间的一场竞赛。如果一方获取了大部分比特币，那么比特币很有可能也就丧失了市场价格和价值。

如果真地出现了量子计算机，并且能破解当前非对称密码系统，那么受到影响的绝不仅仅是一个比特币，而是全球所有的密码和安全保密系统。

100量子位的量子计算机如果来解比特币问题的所有解大概需要多长时间？

本质上讲比特币其实是一种椭圆曲线加密算法，任何加密算法都有被攻破的可能，只是时间长短的问题，以当前的超算可能要几万年，但是量子计算的计算力是惊人的，不需要100位，16位都极有可能短时间内突破，当然，这种突破是历史性的，也意味着银行等金融机构采用的加密算法失效，到人类掌握100位量子的时候也意味着加密算法需要革命性的改变和升级

关于比特币中的量子，比特币 量子的介绍到此结束，希望对大家有所帮助。