基础密码学

在密码算法中，密钥是不可或缺的重要部分，密码算法中的密钥指的是2035547568476535这样一个非常庞大的数字

。无论是执行加密还是解密，都需要密钥。

根据密钥的用法，有对称密码和非对称密码。对称加密指的是使用相同的密钥进行加密和解密。非对称密码需要两个密钥，一个是公钥。另一个是私钥；公钥用于加密，私钥用于解密。公钥可以公开，可以随意发布；私钥可以&#039；不公开，必须由用户本人严格保管。绝不会通过任何方式提供给任何人，也不会透露给想要沟通的信任的对方。

私钥与公钥是如何产生的？

比特币中的私钥是由SHA-256算法生成的32字节(256位)的随机数，相当于一个&quot密码&quot。

，可以证明对比特币地址的完全所有权和控制权。

比特币中的公钥是基于对应的私钥生成的，私钥是由椭圆曲线加密算法生成的一组随机数。椭圆曲线密码算法是不可逆的，也就是说即使公钥暴露，也不会影响私钥的安全性，因为不可能从公钥计算出私钥。公钥主要用于为整个网络中的节点验证事务的有效性。

私钥和公钥是成对生成的，世界上只会有一组，不会重复。

比特币钱包地址是如何产生的？

获得公钥后，公钥被转换为&quot公钥哈希值&quot通过两个哈希函数，这是不可逆的，然后&quot公钥哈希值&quot是通过BASE58编码计算得到的钱包地址。

。钱包地址是这样的：3E1yp8EO5wkaib7drpsftn9xlmu1cizfqg。地址的作用是接收比特币。一个地址收到比特币后，只有拥有相应&quot私钥&quot可以使用它。