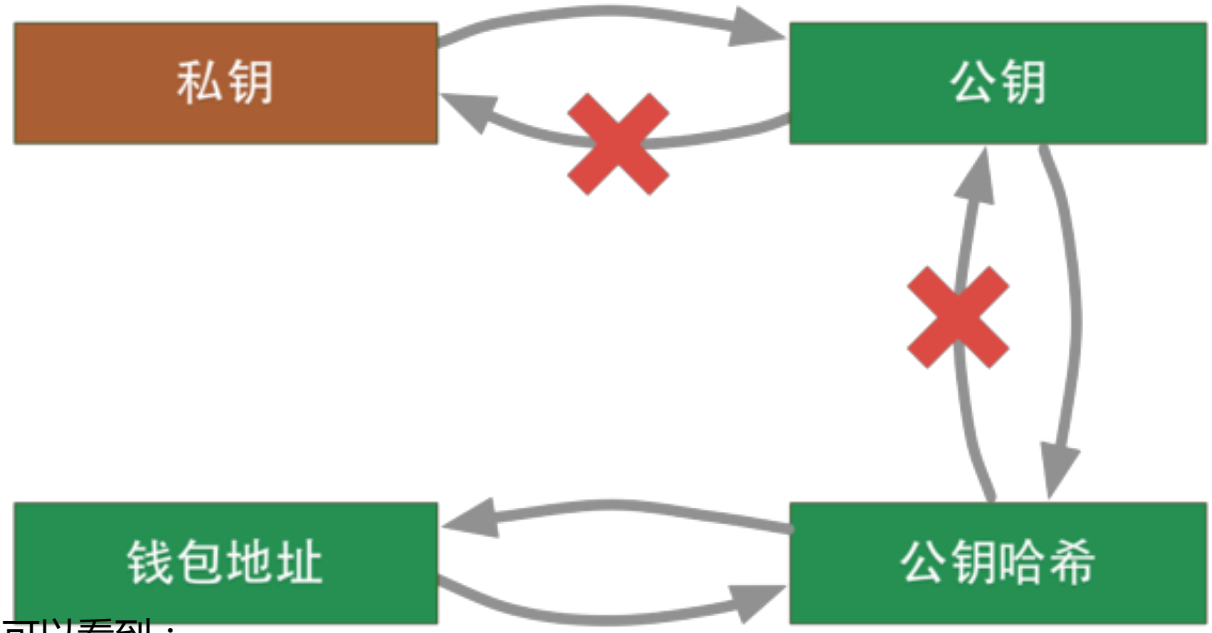
摘要： 比特币私钥、公钥、钱包地址之间的关系

比特币交易涉及到很多密码学知识：公钥、私钥、哈希、对称加密、非对称加密、签名等等。那么哪些是需要用户认真保管不能对外泄露的，那些是需要用户公开的呢？先从钱包地址的生成说起。

钱包地址生成



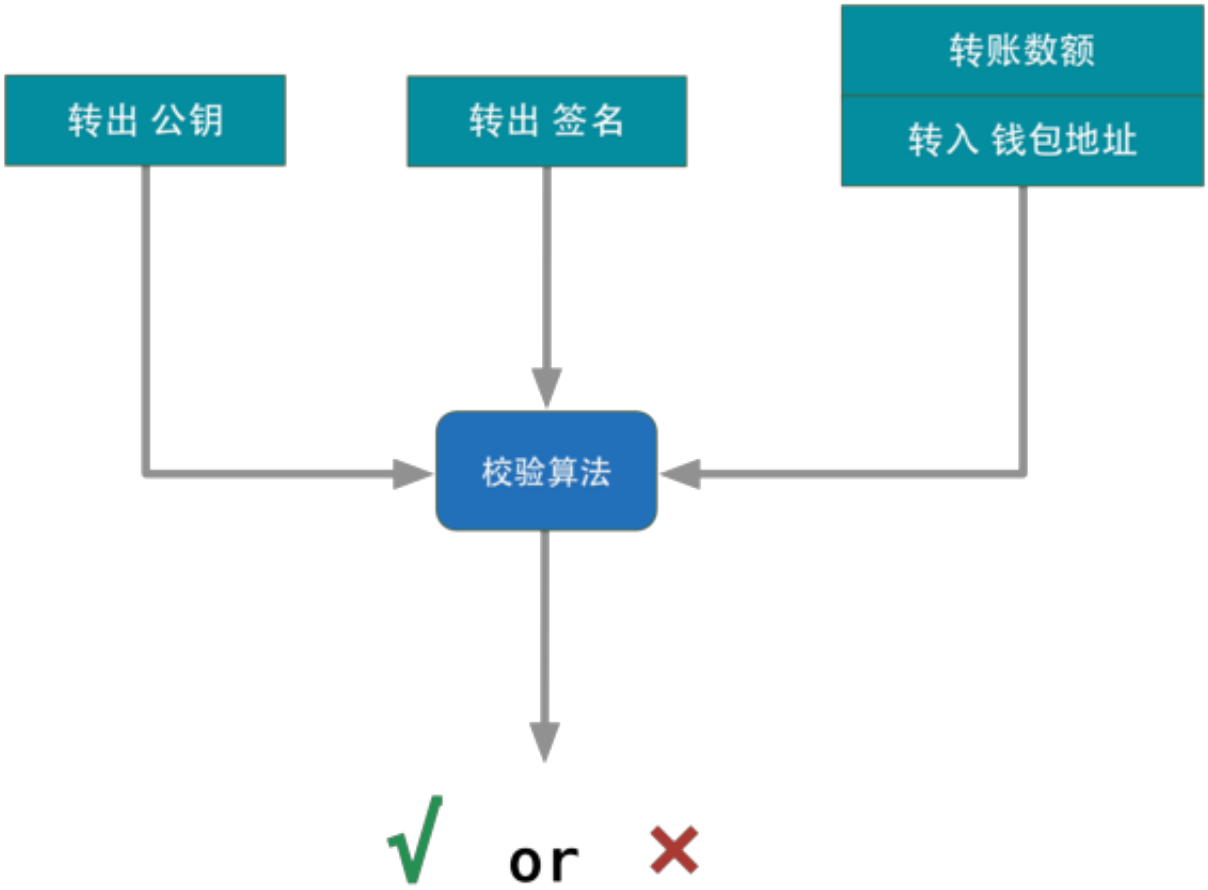
可以看到：

· 通过『私钥』可以得到上述计算过程中所有的值。

· 『公钥哈希』和『钱包地址』可以通过互逆运算进行转换，所以它们是等价的。

使用『私钥』对交易进行签名

比特币钱包间的转账是通过交易（Transaction）实现的。交易数据是由转出钱包『私钥』的所有者生成，也就是说有了『私钥』就可以花费该钱包的比特币余额。生成交易的过程如下：



交易数据被广播到比特币网络后，节点会对这个交易数据进行检验，其中就包括对签名的校验。如果校验正确，那么这笔余额就成功地从“转出钱包”转移到“转入钱包”了。

小结

1.如果一个『钱包地址』从未曾发送余额到其他『钱包地址』，那么它的『公钥』是不会暴露在比特币网络上的。而公钥生成算法（SECP256K1）是不可逆的，即使『公钥』暴露，也很难对『私钥』的安全性造成影响（难易取决于『私钥』的生成算法）。

2.『私钥』用来生成『公钥』和『钱包地址』，也用来对交易进行签名。拥有了『私钥』就是拥有了对这个钱包余额的一切操作权力。所以，保护『私钥』是所有比特币钱包应用最基本也是最重要的功能

（作者：链界社区，内容来自链得得内容开放平台“得得号”；本文仅代表作者观点，不代表链得得官方立场）