有过外贸经历的朋友可能都清楚一种很流行的诈骗手段。骗子会冒充国外客人向国内供货商或者外贸公司发送邮件，用伪造的银行付款水单要求发货，如果没有足够的防范能力和交易原则，就容易中招。更严重的一种方式是黑客侵入与国外客人来往的收件邮箱，冒充自己与国外客人沟通，把本应打给自己的货款截胡到骗子的账号。就我知道的类似事情就发生过很多次，有的损失金额非常巨大。这样的事遇到一次，有些公司就面临倒闭的危险。目前的法律基本上也没有有效的解决方法，因为跨国官司涉及的程序太多，取证困难，成本大，时间长，还不一定有结果。碰到就只能自认倒霉了。

这样的骗局在区块链的世界就更容易避免了，因为我们有保护信息传输的武器。第一个是前天学习的非对称加密，它能保护发送的信息不被篡改。如果我用客人的公钥对发送的信息进行加密，那么只有客人自己才能解密邮件的内容，因为只有他才掌握自己的私钥。但是只保护邮件内容不被他人修改还不够，万一发信的人不是我，而是骗子冒充我。因为区块链中的公钥是公开的，任何人都可以知道客人的公钥。要想验证我才是真正的供货商，收款邮件不是骗子冒充我发的，需要用到另一个武器：数字签名技术。

数字签名的生成过程为：

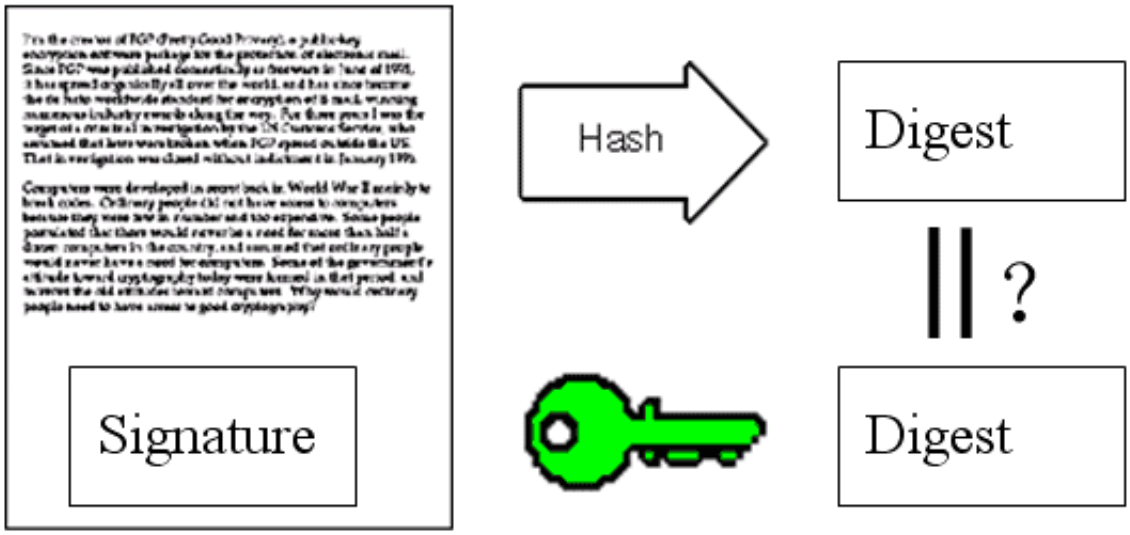
首先是发信人的加密过程

1. 用对方的公钥加密信件原文得到密文M;

2. 用哈希算法计算原文得到哈希值H;

3. 用自己的私钥加密哈希值H得到数字签名S；

4. 把密文M和数字签名S一起发给收信人。



数字签名能够证明我的身份是真实的，因为数字签名是用我自己的私钥进行加密，而私钥只有我自己掌握，别人无法拿到。而且区块链中的私钥算法也很复杂，用现在的技术盗取基本不太可能。

数字签名和非对称加密帮我们验证了两件事:

1. 信息是我发送的，而不是他人伪造的；

2. 信息在发送过程中没有被篡改。

数字签名在区块链中是怎么被应用的？

以比特币的数字签名为例，它是由比特币转账的转出方生成的一段防伪造的字符串，可以用来验证签字者的身份和签字时间，从而证实被签信息是否真实正确。