## **1.比特币地址为什么以1开头？**

答：

Bitcoin地址的生成：  
base58([prefix] + [hash160(pubkey)] + [checksum])  
  
其中,[prefix]1个字节，用于区分不同的网络，如0代表bitcoin的主网络main, 111代表testnet等。  
base58编码实际上就是对一个大整数反复除以58，依次记录余数所对应的base58字符，最后将这些字符逆序，生成一个字符串。  
  
不同网络的[prefix]不同，所以地址首位不同：  
主网络中，［prefix］为0时，除至最后的余数必为0， 对应的base58编码为'1',  所以常规地址的首位一定是'1'.   
testnet中，［prefix]为111， 除至最后的余数为44或45, 对应的base58编码为'm'或'n', 因此testnet网络的地址首位是‘m'或'n'。  
补充：  
多重签名地址用的是script hash, [prefix]为5，base58编码后，地址首位为'3'

