比特币钱包是什么?比特币是一种点对点的电子现金系统，没有实物形态，可以存储在比特币的钱包里，比特币钱包里存储着你的比特币信息，包括比特币地址类似于你的银行卡账号、私钥类似于你的银行卡密码，比特币钱包最核心的作用就是保护你的私钥，可一旦钱包丢失，你就将永远失去这笔比特币。了解完之后回归正题，比特币钱包地址怎么生成获取呢？下面小编给大家详细说说。

比特币钱包地址怎么生成获取？通过随机选出256位二进制数字，形成私钥，然后通过加密函数来生成地址。这个生成方向是单向的。也就是你知道了地址是无法通过解密方法来计算出私钥的。就目前的人类计算机运算能力无法破解，你可以很放心地把地址公布到网上。比特币钱包地址获取操作流程使用随机数发生器生成一个『私钥』。一般来说这是一个256bits的数，拥有了这串数字就可以对相应『钱包地址』中的比特币进行操作，所以必须被安全地保存起来。私钥经过椭圆曲线加密算法(SECP256K1)算法处理生成了公钥，再通过SHA256、RIPEMD160等几种Hash算法计算得到BASE58编码前的钱包地址，这些过程是不可逆的。由公钥可以计算得到公钥哈希，而反过来是行不通的。而使用BASE58(比特币定制版本)，就得到了钱包地址，进行编码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。那么『私钥』、『公钥』、『钱包地址』间的关系是，通过『私钥』可以得到上述计算过程中所有的值，而钱包地址只能拿到公钥哈希。讲完了钱包地址生成过程，回过头看，是甜蛋先转BTC过去的，那怎么使用私钥对交易进行签名，交易数据是由转出钱包的甜蛋A帐户所有者生成，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：1. 交易的原始数据包括“转账数额”和“转入钱包地址”，但是仅有这些是不够的，因为无法证明交易的生成者对“转出钱包地址”余额有动用的权利。所以需要用私钥对原始数据进行签名。2.
生成“转出钱包公钥”，这一过程与生成钱包地址的第2步是一样的。3. 将“转出签名”和“转出公钥”添加到原始交易数据中，生成了正式的交易数据，这样它就可以被广播到比特币网络进行转账了。现在就到了公钥验证的时间，使用公钥对签名进行验证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。最后，小编友情提示，直接通过百度或者谷歌搜索比特币钱包公司的名字，一般可以找到这家公司是什么时候成立的，以及在比特币圈搞了多久，若是是找不到，那干脆别用这个钱包了，不要去相信一个还没有被百度和谷歌收录的比特币钱包公司的产品。