大家好，比特币私钥相信很多的网友都不是很明白，包括比特币私钥破解也是一样，不过没有关系，接下来就来为大家分享关于比特币私钥和比特币私钥破解的一些知识点，大家可以关注收藏，免得下次来找不到哦，下面我们开始吧！

本文目录

私钥探测器已经诞生？比特币的安全性到底有多高？

不知道你说的私钥探测器是啥玩意，但sha256加密算法有简易破解办法的话，不止是比特币废了，密码学都废了。

不过这个社会总有又聪明又勤奋的高手在想着各种办法黑你的钱，比特币私钥也被很多人盯着，毕竟运气好万一暴力破出一个远古钱包，里面放着几万个比特币，别说财务自由，福布斯都可能加上你的名字。

因为通过全节点记录可以知道每个钱包的比特币数量，有针对性的选择一个币多但长期没人登录的钱包能节约一大部分时间，剩下的就只剩破解私钥了。普通人能想到最简单最直接的办法就是暴力破解，虽然概率很小但万一运气好中了呢？

上面是一般人的思路，当然还有更厉害的，有钱包的应该知道，很多私钥自动生成，为了便于记忆会产有助记词，英语单词有多少？助记词的组合排列远比字符的排列组合少多了，原来百万年搞完的活，用助记词碰撞几百年就完事了。

除了上面说的，还有没有其他办法更缩短碰撞的时间，答案是肯定的，光我知道的就还有1-2种办法，我还只是个普通炒币的玩家，那些黑客界没流传出来的办法肯定更多。

所以，世界上没有绝对的安全，只投入性价比，性价比高的话即使再难也有人会想办法去从中牟利（当然就算你几百万刀放一个钱包里，估计黑客也不会想黑你，毕竟没个几亿的回报都可能会亏），咱们普通人能做到的，不要把所有的钱放到一个篮子甚至一个账号里，避免成为别人的猎物。

比特币密钥是保存在硬盘里吗

密钥是钱包生成的一组数据，地址是根据密钥来生成的，而你的地址是用来接收比特币的，所以不用钱包是不能获得密钥的。当然，如果你只是将比特币存在交易平台，那也不需要什么钱包和密钥了。密钥以文件的形式存在钱包文件夹里，所以需要备份这个文件，有人压缩之后放u盘、硬盘、网盘等等。在一个新的电脑上，一个新的比特币钱包，你将你备份的这份密钥文件覆盖这个新钱包的密钥文件，那么这个钱包就显示出你原来的比特币数额了。可以把密钥理解为账号密码的集合，谁有了你的密钥，谁就有了你的比特币。

钱包只是交易的工具，密钥是核心，加密或卸载你的钱包，藏好你的密钥，记住钱包密码，万无一失。

比特币私钥是什么，备份dat后钱包里所有的钱都备份起来了吗？

只要记住私钥就行了。写一张纸上就行。备份什么的无所谓。只要有私钥从任何电脑上将私钥导入钱包你的比特币就可以找回。数量少推荐用比特派钱包。比特派记住十二个汉字就行。12个汉字可以导出私钥。新手还是建议多看论坛。

比特币，以太币钱包的私钥随便改几个数字，会不会刚好是别人的私钥？

首先，要回答这个问题，需要对比特币的公钥私钥和钱包地址，这几个的关系搞清楚。

一、比特币公钥私钥算法

在《比特币：一种点对点的电子现金系统》一文中，中本聪提到了用椭圆加密算法（ECDSA）来产生比特币的私钥和公钥。

基于椭圆加密的原理：私钥是可以计算出公钥的，再由公钥经过一系列数字签名运算就会得到比特币钱包地址。

如下：

私钥——公钥——比特币钱包地址

而比特币中间用到了SHA256加密、RIPEMD160加密和BASE58编码。

二、私钥

私钥就是个随机数，只不过，这个随机数的概率空间很大（256位，也即是2的256次方），什么概念了，你可以数数地球上有多少粒沙子。因此别人是不可能和你生成一样的私钥的（1/2^256的概率），这是比特币甚至整个密码的根基。

三、公钥

而比特币客户端看到的私钥是一串字符串呢？其实这字符串只是私钥进行了Base58校验和编码之后的格式而已。完整过程如图：

经过以上的复杂计算之后，进过11步，Base58编码，就得到了我们经常看到地址了。

oxWoHJrU7VBArBQYhCX9NxHa1RuQat5Bya（编造的，举例用）。

比特币的用户很少会直接看到数字密钥。一般情况下，它们被存储在钱包文件内，由比特币钱包软件进行管理。

四、交易确认

比特币钱包的私钥，作用相当于密码，用于证明比特币的拥有者。拥有者必须使用私密密钥给交易消息签名，以证明消息的发布者是相应比特币地址的所有者。如果没有私钥，用户发送的签名就无法被验证。区块链上账本不会认可该比特币的所有权，用户也就不能使用相应的比特币。

回答问题，也就是说私钥是唯一的，进过计算得到的公钥是唯一的，钱包地址也是唯一的。如果别人拿到了你的私钥，那么他可以计算出公钥，可以生产签名，也就拥有了你的比特币，如果该了私钥刚好是别人的私钥，（几率非常小，因为是随机的，不重复的，空间地址那么大，而且就比特币的私钥量来说，也只是占随机私钥地址空间很小很小很小的部分。打个比方：就相当于整个私钥空间是地球所有的沙子这么大，每一粒沙子唯一标识，而比特币私钥只使用了你脚底下那么一点沙子，你随便改一个，可能改到上海某地的一粒沙子上了，而不是你脚底下的某粒沙子。而那样的沙子地下是没有比特币的），而如果没有备份私钥，改了之后，你无法找到私钥，那么你将永远失去这个私钥下的比特币。

码字不容易啊，各位看官请点赞+关注。更多互联网专业内容。

比特币私钥和比特币私钥破解的问题分享结束啦，以上的文章解决了您的问题吗？欢迎您下次再来哦！