

比特币赎金被美国政府追回，比特币还可信吗？

6月8日，数字货币再度重挫，过去24小时内，比特币暴跌近10%，以太坊、瑞波币等跌幅均超10%。不少网友们对此热议，并对比特币产生了质疑。美国科洛尼尔管道运输公司（ ）上月遭黑客袭击勒索。公司被黑客袭击后被迫全面暂停运营，17个州及华盛顿特区一度进入紧急状态。黑客收到付款后提供了解密工具帮助恢复其计算机网络。“今天我们扭转了局势，”摩纳哥在发布会上称，“我们将继续使用所有工具所有、获取到了私钥。



再请教一个比太钱包的问题。谢谢

用旧手机下了比太钱包离线生成了HD账户。比如我想从某交易所提比特币到这个冷钱包，)谢谢这不简单，文字识别，提取地址。你不能用手机上请教一下，比太钱包HD冷账户里有比特币，但是热监控里看不见余额。比太钱包HD冷账户有比特币，但是热监控里也看不见余额，点发送也是显示“余额为零，无法发送”。应该是生成发币二维码，用冷钱包扫描签名后，生成已换手机如何克隆热钱包。用新手机下载了一个比太，克隆是不是在高级选项中“来自比太私钥二维码，来自私钥明文，来自HD种子二维码，来自HD密语”导入即可啊，导入后要不要在扫一下冷钱包监控，各位老大不知道，



### “比特币之父” 中本聪身份之谜

2008年早些时候，曾向克莱曼寻求帮助。起诉书中称，二人合作完成了那篇文章，并共同创造了比特币。比特币融合了加密技术、分布式计算和博弈论。有了比特币，就可以在几分钟之内进行交易，而无需借助中间方。每一笔比特币交易中都有两串数字，一串是公钥，另一串是私钥。任何人都可以将比特币发送至公钥，或是目标地址，这类似于银行账户。但只有账户户主才知道私钥，可以真正拥有比特币。比特币发展初期，比特币没有有形价值，支持者也只有寥寥数人。后来大约有两年时间，不仅在网络留言板上写文章，还时常给开发人员发电子邮件。2010年12月，这个人好像突然消失了。而当时据外界所知，此人会使用两个电子邮箱，还注册过一个网站。



### 区块链与量子力学本质上都是科学

当量子力学与电子计算机相遇,于是就诞生了量子计算机。量子计算机出来之后,比特币马上被攻克,您如何看待这些言论。区块链是数学、未来它到底为人类能做出何种贡献,还需要时间来证明。关于量子计算机可以攻克比特币体系、秒杀区块链这些言论,在我看来是反科学观点。目前还处于理论状态,即使量子计算机被研发成功可以商用,它不只是威胁比特币,如果当量子计算机能被人类大范围使用时,



### 比特币大跌会崩盘吗

在讨论比特币会不会大跌导致崩盘之前，变成一张废纸，那么这种情况有可能发生。或者计算机技术突飞猛进，量子计算机能够现实应用并且计算能力提高很多（例如 $10^{10}$ ）倍，这也导致比特币体系不可靠。或者如果全球政府一齐禁止交易比特币，交易速度、那么商业前景也会受到影响。但是发生概率很小。后一种问题发生概率略大，但是不致命，



私钥和地址从哪来？

然后通过手工计算来算出地址。通过抛硬币将正面向上计为0，反面向上计为1，连续抛256次，这个数字就是私钥。这个随机性有多随机呢。就是不可能出现相同。让计算机去抛硬币来碰私钥，所以这样私钥只要生成出来，那它就可以被用来标识所有权而不用担心和别人重复。有了私钥，就可以通过加密函数来生成地址。公布到网上。但千万别把私钥透露给别人，