大家好，关于比特币钱包秘钥很多朋友都还不太明白，不过没关系，因为今天小编就来为大家分享关于未来量子计算机可否用来破解比特币的秘钥？的知识点，相信应该可以解决大家的一些困惑和问题，如果碰巧可以解决您的问题，还望关注下本站哦，希望对各位有所帮助！

本文目录

未来量子计算机可否用来破解比特币的秘钥？

未来的理想通用型量子计算机完全有可能破解比特币。不过一旦破解，比持币其存在价值将大打折扣，现在其之所以有价值，是因为只有极少数人可以操控玩弄，方显价值之珍贵，其本属虚拟而非实物，某种情况下可以变得一文不值。谢邀，答毕。

加密货币如何加密？

所谓加密货币是指以密码学为基础的匿名货币体系。

简单来说，是通过密码学来保障虚拟货币的匿名性，和价值转移特性。

匿名性是通过非对称加密方式来实现，也就是说每个资产有两个秘钥，公钥和私钥。公钥关联资产，私钥保存在个人手中。个人通过私钥签名，大家通过公钥验证就可以转移资产。因为私钥和公钥可以无限增加，也不署名，所以就可以实现匿名性。

价值转移是指一笔钱花了之后就会转移到别人手中，不会再在自己手中，也就是不会有一笔钱花两次的问题，（双花问题）。比特币中是采用密码学中的哈希运算进行工作量证明，再加上可以追踪的utxo方式可以解决这个问题。

因为大量采用加密学的技术，所以就会称为加密货币，或匿名货币。

比特币是数字货币吗？

谢谢悟空问答的邀请！

首先简答：不是！

长久关注我的网友都知道我对比特币一以贯之的观点了，特别在10月15日，以“加密货币是不是值得持有的资产？”为题，我作为反方，与正方、前中金公司财富执行总经理吴小平，在百度《超级对线》做了一场PK直播，吸引了120多万人观看。一开始，就激辩了未来比特币是否能会成为世界货币，我观点鲜明：不会！

请收看回放，里面详谈了几乎所有和比特币相关问题。

既然又被问到了，再谈几句吧。

这样说吧，真正的数字货币是有价值的，个人认为今后只会有一种真正的数字货币：国家背书的各个国家达成共识的数字货币，受理环境比目前的信用卡VISA、支付工具PayPal等更简单、成本更低、更安全，无网有网均可使用。

而比特币、以太坊、火币等并不能叫数字货币，因为他们不具备，货币的基本流通属性，离开互联网就无法证明其存在与交易了，最多叫数字符号或电子符号，只是虚拟币而已！

有网友不断问及，当下投资什么最好，其实，之前我反复强调了：当下现金为王。

借着这个问题，再顺便谈一下，与股票和债券相比，其实，现金并非一无是处。

当下，股票估值普遍高得令人难以置信，但投资者通常用来给投资组合提供保护的长期国债价格高得令人震惊。在这种情况下，更好的对冲方式可能是老式方法：持有现金。

几乎从任何角度来看，股票估值看起来都相当高。如，标普500指数基于未来一年收益预期的市盈率为22倍，为互联网泡沫以来最高的预期市盈率。与其过去十年经通胀调整后的收益（由经济学家RobertShiller推广的估值方法）相比，估值也同样偏高。美国股市总价值与国内生产总值(GDP)之比等其他衡量标准显示的结果也类似……

总之，比特币不是数字货币……点到为止吧。

最后，再顺便打个小广告，《看懂货币的第一本书》新鲜出炉，谢谢关注！

你对这个问题有什么更好的意见吗？欢迎在下方留言讨论！

FBI查封DarkSide勒索款，比特币私钥真的被攻破了吗？

FBI攻破比特币密钥目前还是很有难度的。不过如果拿到密钥那就简单多了，千万不要低估FBI的实力。据悉，联邦调查局(FBI)掌握了一把私人密钥，可以解锁一个收到了大部分赎金的比特币钱包。目前还不清楚FBI是如何获得该密钥的。

关于本次比特币钱包秘钥和未来量子计算机可否用来破解比特币的秘钥？的问题分享到这里就结束了，如果解决了您的问题，我们非常高兴。