比特币如何抗量子-
量子计算机会不会从根本上击垮比特币?-股识吧

一、为什么说量子计算机可轻易破解比特币，究竟怎么

摘要：在位于纽约市以北约50英里处僻静乡村中的一个小型实验室内，天花板下缠绕着错综复杂的管线和电子设备。
这一堆看似杂乱无章的设备是一台计算机。
它与世界上的任何一台计算机都有所不同，而是一个即将开创历史的里程碑式设备---量子计算机。
2022年5月3日，科技界的一则重磅消息：世界上第一台超越早期经典计算机的光量子计算机诞生。
这个“ 世界首台 ”是货真价实的“ 中国造 ”，属中国科学技术大学潘建伟教授及其同事等，联合浙江大学王浩华教授研究组攻关突破的成果。
如果现在传统计算机的速度是自行车，量子计算机的速度就好比飞机。
在过去的几个月里，IBM和英特尔已经宣布他们已经分别制造了50和49个量子比特的量子计算机。
有专家指出，在十年之内，量子计算机的计算能力就可能赶超当前的超级计算机。
2022年3月5日在洛杉矶举行的美国物理学年会上，谷歌量子AI实验室研究科学家Julian Kelly报告了，带领谷歌团队正测试一台72量子比特通用量子计算机。
然而，这还是仅仅是72量子比特而已。
按照这个速度发展下去，很快量子计算机的神通，将强劲得让人恐惧。
那么，为什么说量子计算机可轻易破解比特币，究竟怎么回事？要破解现在常用的一个RSA密码系统，用当前最大、最好超级计算机需要花60万年，但用一个有相当储存功能的量子计算机，则只需花上不到3个小时！也就是说，从电子计算机飞跃到量子计算机，整个人类计算能力、处理大数据的能力，就将出现上千上万乃至上亿次的提升。
在量子计算机面前，我们曾经引以为豪的传统电子计算机，就相当于以前的算盘，显得笨重又古老！虽然比特币协议使用的是不对称的加密货币，用相应的公钥验证私钥签署的交易，以确保比特币只能被合法所有人使用。
使用当前可用计算机强制私钥与公钥保持一致不可行，但量子计算机却可以解决不对称加密货币的问题。
另外，比特币的规定是处理得更多的那个区块加入区块链，另一个区块则作废。
举个例子，这就像于在一个账簿里有51个人说你在银行存了100块钱，而49个人说你存了50块钱，这种情况下，区块链算法少数服从多数，银行认为你存了100块钱是真，存了50块钱是假。
所以一旦一位矿工拥有51%的算力，其他后续矿工将无法继续获得比特币。

Andersen Cheng，英国一家网络安全公司的联合创始人，他表示在量子计算机投入使用的那一天，比特币就会终结。
你觉得呢？

二、量子计算机会不会从根本上击垮比特币?

其实量子计算机对比特币的威胁不在于挖矿，而在于对交易的攻击。
我们知道，比特币的交易是由去中心化的密码学认证完成的，而这个认证方式的核心是散列算法。
如果有量子计算机的话，可以制造碰撞(Grover算法，多项式加速)，用以伪造交易从而获利。
而因为比特币的核心算法已经固定，如果不改变算法的话，无法增加密钥长度，也就无法抵御这种攻击。
不过，有实用的量子计算机的话，干啥不比搞这种攻击强……满意请采纳

三、为什么说比特币是不能破解的，用量子计算机也不行？

最近GOOGLE那边有消息，还特意找了一个量子力学专家验证，目前所谓的量子计算机还没达到媒体宣传到的那种效果，所以量子计算机技术成熟肯定还需要一段时间，再等几年吧

四、北京比较有名的牛皮癣医院?北京东方建都医院怎么样?

我来回 记得有个朋友是得了牛皮癣，好几年了，前段时候是听说去北京看了，现在好了，采用牛皮癣“ 6A量子 ”抗复发体系，搜索了下是北京东方建都医院的疗法，我想着应该不错，电视上也经常看到东方建都医院的广告！

五、量子计算是对比特币的威胁吗？

是的，包括传统银行系统在内的大部分依赖于密码学的系统都是这样。
但是量子计算机还不存在，也许短期内也不会出现。

当量子计算确实即将成为比特币威胁的时候，可以利用后量子算法来更新比特币协议。
基于这一更新的重要性，有理由相信开发人员会将其反复审核，最终为所有比特币用户接受

六、为什么说比特币是不能破解的，用量子计算机也不行？

随着量子计算机出现，用量子计算机的量子攻击可以解决底层数学问题，加密货币的安全基础就不复存在。
加密货币有必要开始着手推进抗量子攻击的方案。
ABE/艾比币为了对抗量子攻击，升级现有的加密算法，将椭圆曲线密码技术升级为格密码技术。

七、为什么需要抗量子攻击的加密货币?

随着量子计算机出现，用量子计算机的量子攻击可以解决底层数学问题，加密货币的安全基础就不复存在。
加密货币有必要开始着手推进抗量子攻击的方案。
ABE/艾比币为了对抗量子攻击，升级现有的加密算法，将椭圆曲线密码技术升级为格密码技术。

参考文档