量子计算机凭什么能干掉比特币——如何抵抗量子计算机的攻击-股识吧

一、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

二、利用超级计算机挖比特币是赔还是赚

当然是赔了！以前就是有个美国的家伙利用职务之便用超级计算机挖，结果被发现……据说得的钱也就那么点，连电费的十分之一都不够！

三、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

四、量子计算机这块快可以挖矿吗

这货大植物大战僵尸一定非常给力！

五、【R】【提问：量子计算机会让整个Bitcoin系统崩盘么？】

量子电脑会让黑客更轻易攻击比特币的钱包，盗取里面的比特币。
量子计算机可以进行大数的因式分解，和破译密码，但是同时也提供了另一种保密通讯的方式。
正所谓解铃还需系铃人，量子通讯才是真正不会被破解的保密通讯比特币的密码系统是可以改进成量子通讯系统的。
当然，量子电脑短期内还不会出现。

六、如何抵抗量子计算机的攻击

就算有量子计算机，破解比特币也不是那么容易的事，基本不具实际可行价值。
况且已经有更好的方案提出可让BTC更加安全的抵御量子攻击，可以在必要时加入。
你可以参考一下这个文章：*：//bitcoinmagazine*/6021/ ... and-how-we-can-fix/

七、什么是数字货币中的量子攻击?

数字货币的一个关键技术就是椭圆曲线加密，它是目前加密货币数字签名的核心技术，能确保加密货币的所有权、不可复制以及交易的完整性。
但随着量子计算机出现，它将不再安全。
用量子计算机的量子攻击可以解决底层数学问题，基于椭圆曲线加密的数字签名可能是可以伪造的。
这对于加密货币来说是致命的，因为分布式账本的记录是不可篡改和逆转，如果椭圆曲线加密能够被攻破，那么加密货币的安全基础就不复存在。

八、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

参考文档

下载：量子计算机凭什么能干掉比特币.pdf
《小规模纳税人印花税零申报怎么报》
《000021这只股票怎么样》
《股票主力操盘和散户有什么不同》
《通货膨胀环境下买什么股票》
下载：量子计算机凭什么能干掉比特币.doc
更多关于《量子计算机凭什么能干掉比特币》的文档...

声明：
本文来自网络，不代表
【股识吧】立场，转载请注明出处：
https://www.gupiaozhishiba.com/article/70597070.html