比特币为什么面临量子计算的挑战：量子计算是对比特币的威胁吗？-股识吧

一、比特币是用户通过电脑解决一个特定数学问题而得到的奖励，数学问题那么为什么它数量有限？

首先这个数学问题其实就是个猜随机数的游戏，比特币系统是出题者，矿工是答题者，矿工在不停地用猜的随机数去计算哈希值，直到满足比特币系统出题的要求，而比特币系统是中本聪开发的，他将题目数量设置了上限，故而是有限的，这样比特币的数量也就是有限的

二、为什么挖掘比特币需要大量计算?

比特币(BitCoin)是一种P2P形式的数字货币。
点对点的传输意味着一个去中心化的支付系统。
比特币不依靠特定货币机构发行，它依据特定算 法，通过大量的计算产生，比特币经济使用整个P2P网络中众多节点构成的分布式数据库来确认并记录所有的交易行为。
P2P的去中心化特性与算法本身可以确保无法通过大量制造比特币来人为操控币值。
基于密码学的设计可以使比特币只能被真实的拥有者转移或支付。
这同样确保了货币所有权与流通交易的匿名性。
比特币是一种网络虚拟货币，数量有限，跟腾讯公司的Q币类似，但是可以用来套现：可以兑换成大多数国家的货币。
比特币与其他虚拟货币最大的不同，是其总数量是非常有限的，具有极强的稀缺性。
该货币系统在前4年内只有不超过1050万个，之后的总数量将被永久限制在2100万个之内。
还有一点是，你可以用电脑生产比特币

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

五、比特币说的是计算的特定数学问题到底是什么问题？那个数学问题有什么用啊？？求解啊

所谓的计算特定数学问题(挖矿)，其实是在生成 block (一种用于维护 比特币 系统的安全性的机制). 它所涉及的密码学本质导致它越来越难算.这个计算与其他的分布计算项目没有任何关系， 只是一种用于内部的计算， 只是为了维护 比特币 系统的安全性.原文：The computations done when mining are internal to Bitcoin and not related to any other distributed computing projects. They serve the purpose of securing the Bitcoin network， which is useful.

六、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

七、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

八、问几个关于比特币的问题，比特币计算的到底是什么东西；算出来有什么价值，为什么说发行量只有2100万？

网络虚拟货币。
可以代替现实的钱来使用。
。
不过。
中国银行不承认这款

参考文档