量子计算与比特币是什么东西－比特币是什么东西-股识吧

一、量子计算机的出现会对比特币造成威胁吗

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

二、求问大神比特币的算力说的是什么意思？

计算能力 一般显卡Mh/s 专业矿机Gh/s比特币挖矿靠的就是计算能力计算能力越快比特币挖的就越快

三、量子计算机是个什么玩意

量子计算机（quantum computer）是一类遵循量子力学规律进行高速数学和逻辑运算、存储及处理量子信息的物理装置。
当某个装置处理和计算的是量子信息，运行的是量子算法时，它就是量子计算机。
量子计算机的概念源于对可逆计算机的研究。
研究可逆计算机的目的是为了解决计算机中的能耗问题。
详情请参照股票百科。

四、什么是量子计算

量子计算 (quantum computation) 的概念最早由IBM的科学家R. Landauer及C. Bennett于70年代提出。

他们主要探讨的是计算过程中诸如自由能(free energy)、信息(informations)与可逆性(reversibility)之间的关系。
80年代初期，阿岗国家实验室的P. Benioff首先提出二能阶的量子系统可以用来仿真数字计算；
稍后费因曼也对这个问题产生兴趣而着手研究，并在1981年于麻省理工学院举行的First Conference on Physics of Computation中给了一场演讲，勾勒出以量子现象实现计算的愿景。
1985年，牛津大学的D. Deutsch提出量子图林机(quantum Turing machine)的概念，量子计算才开始具备了数学的基本型式。
然而上述的量子计算研究多半局限于探讨计算的物理本质，还停留在相当抽象的层次，尚未进一步跨入发展算法的阶段。
1994年，贝尔实验室的应用数学家P. Shor指出 [3]，相对于传统电子计算器，利用量子计算可以在更短的时间内将一个很大的整数分解成质因子的乘积。
这个结论开启量子计算的一个新阶段：有别于传统计算法则的量子算法(quantum algorithm)确实有其实用性，绝非科学家口袋中的戏法。
自此之后，新的量子算法陆续的被提出来，而物理学家接下来所面临的重要的课题之一，就是如何去建造一部真正的量子计算器，来执行这些量子算法。
许多量子系统都曾被点名做为量子计算器的基础架构，例如光子的偏振(photon polarization)、空腔量子电动力学(cavity quantum electrodynamics, CQED)、离子阱(ion trap)以及核磁共振(nuclear magnetic resonance， NMR)等等。
以目前的技术来看，这其中以离子阱与核磁共振最具可行性。
事实上，核磁共振已经在这场竞赛中先驰得点：以I. Chuang为首的IBM研究团队在2002年的春天，成功地在一个人工合成的分子中(内含7个量子位)利用NMR完成N=15的因子分解(factorization)

五、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

六、比特币是什么东西

比特币没有一个集中的发行方，而是由网络节点的计算生成，谁都有可能参与制造比特币，而且可以全世界流通，可以在任意一台接入互联网的电脑上买卖，不管身

处何方，任何人都可以挖掘、购买、出售或收取比特币，并且在交易过程中外人无法辨认用户身份信息。

七、de=1modφ(n)是什么意思

在RSA算法中，de=1modφ(n)是指de与1关于φ(n)同余。
对极大整数做因数分解的难度决定了RSA算法的可靠性。
对一极大整数做因数分解愈困难，RSA算法愈可靠。
假如有人找到一种快速因数分解的算法的话，那么用RSA加密的信息的可靠性就肯定会极度下降。
但找到这样的算法的可能性是非常小的。
只有短的RSA钥匙才可能被强力方式解破。
世界上还没有任何可靠的攻击RSA算法的方式。
只要其钥匙的长度足够长，用RSA加密的信息实际上是不能被解破的。
扩展资料：由于RSA算法基于大数分解（无法抵抗穷举攻击），因此在未来量子计算能对RSA算法构成较大的威胁。
一个拥有N量子比特的量子计算机，每次可进行2^N次运算，理论上讲，密钥为1024位长的RSA算法，用一台512量子比特位的量子计算机在1秒内即可破解。
1983年麻省理工学院在美国为RSA算法申请了专利。
这个专利2000年9月21日失效。
由于该算法在申请专利前就已经被发表了，在世界上大多数其它地区这个专利权不被承认。
参考资料来源：股票百科-RSA算法

八、比特币的概念是什么？为什么通过计算产生的比特币会有价值？

比特币没有一个集中的发行方，而是由网络节点的计算生成，谁都有可能参与制造比特币，而且可以全世界流通，可以在任意一台接入互联网的电脑上买卖，不管身处何方，任何人都可以挖掘、购买、出售或收取比特币，并且在交易过程中外人无法辨认用户身份信息。

参考文档

下载：量子计算与比特币是什么东西.pdf
《联科科技股票中签后多久不能卖》
《股票开户最快多久能到账》
《场内股票赎回需要多久》
下载：量子计算与比特币是什么东西.doc
更多关于《量子计算与比特币是什么东西》的文档...