很多朋友对于量子计算机区块链和区块链不太懂，今天就由小编来为大家分享，希望可以帮助到大家，下面一起来看看吧！

本文目录

“区块链在量子计算机面前一文不值”是真的吗？

作为一名科技工作者，我来回答一下这个问题。

首先，在谈论技术的时候一定离不开当前的技术大环境，在当前的技术环境下，量子计算机还仅仅处在研发的初期（或者叫构想更确切一些），甚至连基本的架构还处在探讨当中，所以量子计算机未来很长一段时间内仅仅是一个研究方向，要想实现应用还需要很长一段路要走，因为这涉及到技术体系的重构，是一个庞大的工程。

区块链目前与量子计算机相比，是两个时代的对比，就像冷兵器时代的武器与现代武器对比一样，可以看成是一种“维度上”的差距，但是也并不是说未来在量子计算机时代，目前所有的技术都没有意义了，只不过整个技术体系都会有新的解决方案，传统方案往往只成为了一种备用方案而已。

从当前的技术体系结构来看，目前区块链技术具有非常重大的发展意义，采用区块链技术不仅能够解决当前大量的实际问题，同时也能够在一定程度上推动产业结构升级，所以目前探讨区块链技术更有实际意义。至于未来区块链技术是否会被淘汰，并不是现在应该关心的核心问题，从大的发展方向来说，没有一个技术是不会被淘汰的。

当前大数据、物联网、云计算和人工智能等技术都处在落地应用的初期，除了云计算的应用相对比较顺利之外，其他技术体系的落地应用还需要破除一系列行业壁垒，而区块链技术能够在一定程度上解决这个问题，所以目前区块链领域也是一个创新的热点领域。从当前大的发展趋势来看，区块链与大数据的结合将有很多创新点，也能够打开新的价值空间。

我从事互联网行业多年，目前也在带计算机专业的研究生，主要的研究方向集中在大数据和人工智能领域，我会陆续写一些关于互联网技术方面的文章，感兴趣的朋

友可以关注我，相信一定会有所收获。

如果有互联网、大数据、人工智能等方面的问题，或者是考研方面的问题，都可以在评论区留言，或者私信我！

任正非曾经说在量子计算面前，区块链就是小儿科，真的是这样吗？

谢谢您的问题。任正非先生关于量子计算和区块链的言论，是有一定道理的。

量子计算机不是普通计算机。虽然都是处理数据和解决问题，量子计算机运用的是量子力学理论，不属于传统计算机的范畴。量子计算机通过量子位的叠加与交织，执行大量的计算工作。超强的计算能力，是解决很多问题的基础。

量子计算机和会威胁到区块链。两次计算机可以通过强大的计算资源和算力，破解区块链加密，这有可能就是任正非说的本意。区块链加密目前是很安全的，但是多数区块链ECDSA密钥创建标准，有可能被量子计算机破解公钥和密钥的关系，从公钥要获得密钥，毕竟公钥眼下是安全共享的，量子计算机可以以此为突破口。

量子计算也许没有那么广的实用性。量子计算之前需要大量充分的数据准备工作，将传统意义上的数据转化为量子计算所需的数据，这个过程非常精细繁琐、不容差错。所以量子计算用于特定、重大计算任务非常有效，普遍使用还不太成熟。从这个意义上说，量子计算和区块链并非水火不容，各有用途罢了。

欢迎关注，批评指正。

任正非近日说区块链在量子计算面前没多大用，如何评价？

区块链准确的称谓应当是分布式账本，它的特点之一是账本的不可篡改性，而这个不可篡改性是基于计算的难度的，和比特币的“挖矿”属于同性质，而量子计算得以应用的话，分布式账本的不可篡改性顷刻间便土崩瓦解了，故在理论上，任正非说的有道理！????

量子计算机一旦突破，可以破解区块链么？

技术进步的速度永远快过人们的想象。近来不仅世界时局变幻，连加密领域都迎来了当头一激灵。9月21日发布在NASA后又被火速删除的谷歌论文，甚至轰动了国际朝野。论文表明，谷歌研发的量子计算机用3分20秒完成的一项计算，全球最强大的超算Summit计算机则需要花1万年。由此实现量子霸权。

量子霸权，也叫量子优势，即在未来的某个时刻，功能强大的量子计算机可以完成经典计算机几乎不可能完成的任务。谷歌说：这标志了第一个只能用量子处理器执行的运算。在通往全面量子计算的路上，这是一个里程碑。量子机器的算力，将会以双指数速度增长。

看似一夜之间，我们的生活进入量子信息时代。让我们先来搞清楚量子计算机有何过人之处。

量子电脑的概念是在1982年由物理学家费曼（RichardFeynman）首先提出，12年之后，数学家PeterShor建立了演算法，受到更多科学家的重视。传统电脑是用二进位的位元（bit）运算，仅有两个状态：0和1，不会有其他状态。量子位元却有介于0和1之间的状态。

根据薛丁格的理论，在一个系统被观测之前，它的状态不会是个确切的数值，而是机率函数的叠加状态。这个理论是量子力学的基础，也是量子电脑的原理。量子电脑的位元会是0和1的机率叠加状态，这让量子电脑有更多元的状态可以做运算，因此运算速度加快。

来自谷歌量子人工智能实验室的负责人HartmutNeven认为，量子计算机比经典计算机存在着两个指数优势：首先，量子位相比普通位具有效率优势，如果一个量子电路具有4个量子位，那么需要一个具有16个普通位的经典电路才能实现等效的计算能力。其次，量子芯片也在快速改进。谷歌量子芯片正在以指数级的速度发展，这种快速的改善是由于量子电路中错误率的降低。而降低错误率能帮助我们构建更大的量子芯片。双指数的增长速度远远快于指数函数，因此谷歌认为虽然量子计算机速度现在远不及经典计算机，但是总有一天会超过后者。

而这代表了什么呢？

其一，如果进入实用，可以实现数百个量子比特相干操纵的专用型量子计算系统，应用于具有实用价值的组合优化，量子化学，机器学习等方面，指导新材料设计，药物研发等。波士顿咨询（BCG）援引部分制药行业的高管预估，量子模拟可将药物发现率提高5%-10%，并节省15%-20%的研发时间。其二，进入到通用可编程的量子计算机阶段，能够相干操纵数亿量子比特，实现可容错的量子计算机，能在经典密码破解，大数据搜索，人工智能等方面发挥巨大作用。

这造成了加密世界极大的恐慌，业界纷纷评论，区块链技术面临极大被取代的威胁，加密货币将毫无价值。未来若是量子电脑发展完备，就有可能在几秒钟的时间内，破解现有的公钥系统密码，包含银行系统、比特币等密码货币的数位签章。而早在2017年，新加坡国立大学的研究人员及其同事就已经开始关注量子计算机可能在

多长时间之内就能破坏比特币的安全性。

那实际情况又是如何呢？

根据美国加密货币研究与工程中心的研究论文表示，一台量子电脑至少要包含1500个量子位元，才能够进行Shor演算法。对比目前Google所发现的Sycamore，也仅设计了54个位元，就算加上谷歌测试名为「Bristlecone」的量子计算机，目前也只拥有72个量子位元；含1500个量子位元的电脑可能仍需数年才能诞生。

加之，量子计算机的实际应用也面临诸多问题。由于在于0和1两种状态之间的能量差太小，需要降低到绝对零度附近，才能防止被热量所破坏。

此外，粒子之间状态的耦合也有时间限制，时间一长，两个粒子将不再“相干”。在进行量子计算实验时，所有的量子操作要在量子退相干之前完成，才能保证量子操作的保真度（Fidelity），否则运算结果将不再可信。

所以，现在就恐慌怕是为时尚早。区块链除了加密这项技术外，背后还有更多复杂的设计，想要取代并非是可以延续所有区块链优点的升级换代。哪怕是密钥可以被瞬间破解的时刻到来，那么区块链所寓意的“公平，无边际信任”又是否可以被量子信息时代所保证呢？人性又是否可以随着量子霸权进化为不需要“信任”来做自我防御的本能了呢？那时的生命财产安全，又该如何保护呢？

关于量子计算机区块链的内容到此结束，希望对大家有所帮助。