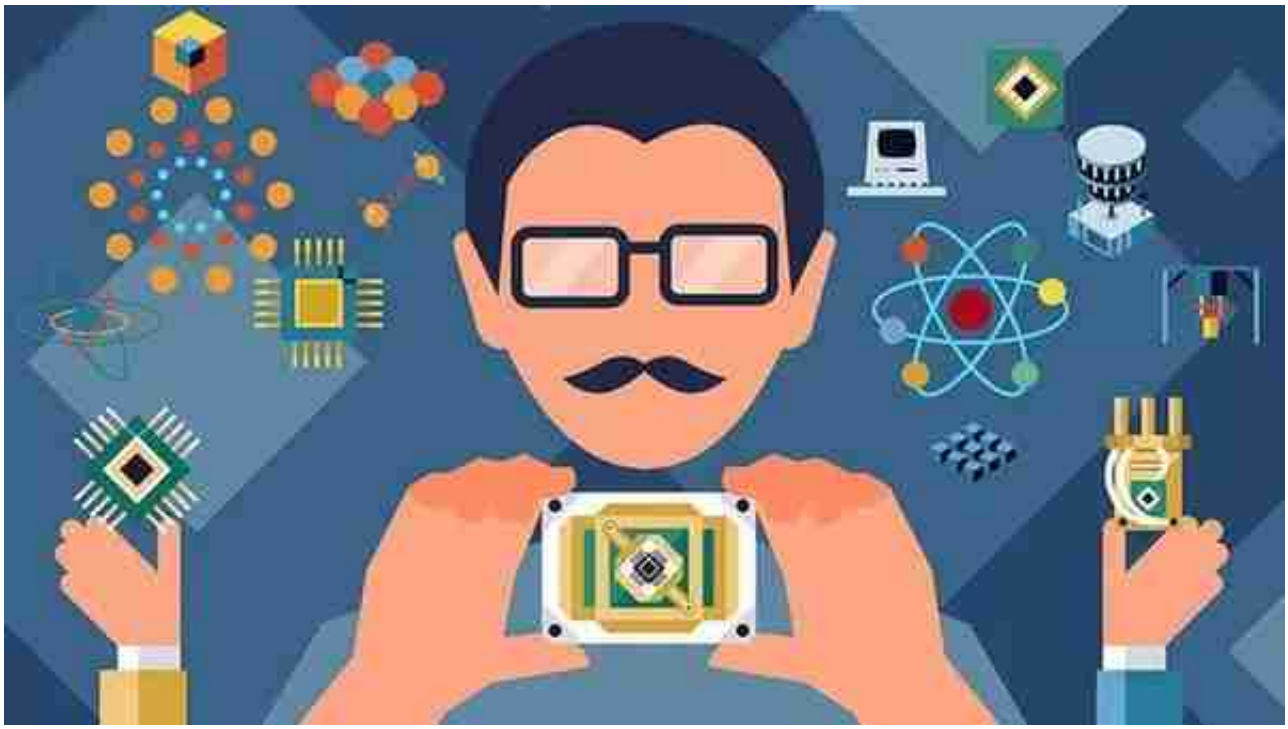
2019年CES大会上IBM宣布推出被誉为杀手锏的目前全球第一台独立商用量子计算机IBM Q System One。IBM称Q System One
是「世界上首款专为科研和商业用途设计的全集成通用量子计算机」，它可以操纵20 个量子比特。虽然目前量子计算机的计算力可能还比不过一台笔记本，不过它的出现还是掀起了一番热潮，证明了量子计算机可以走出实验室环境，把大众脑海中虚幻的想象以实体呈现出来。

量子计算机的运算采用了量子力学原理，对于传统计算机来说非常耗时的一些问题，它能够以少得多的步骤找到解决方案。众所周知，区块链依赖的加密算法在现有算力下是难以破解的，不过量子计算机的运行原理和传统计算机完全不同，根据MIT技术评测报告，量子计算机可以攻破区块链加密算法，从而威胁整个区块链世界的安全。

世界上已经有很多专家提出量子计算机会威胁区块链和加密货币安全的观点，这也是目前区块链技术的一个重要议题。IBM量子计算机部门的相关人士在年初也警告说，实际上这种威胁迫在眉睫，应该尽早采取应对措施。



作为走在量子计算机和区块链技术最前沿的公司之一，IBM的观点显然非常具有参考性，在2月份举办的“IBM Think 2019”大会中，IBM高管讨论了量子计算机对虚拟货币和区块链的威胁，IBM的区块链和数字货币业务副总裁Jesse Lund警告说，量子计算机有可能对虚拟货币的钱包和密钥产生严重的安全威胁。

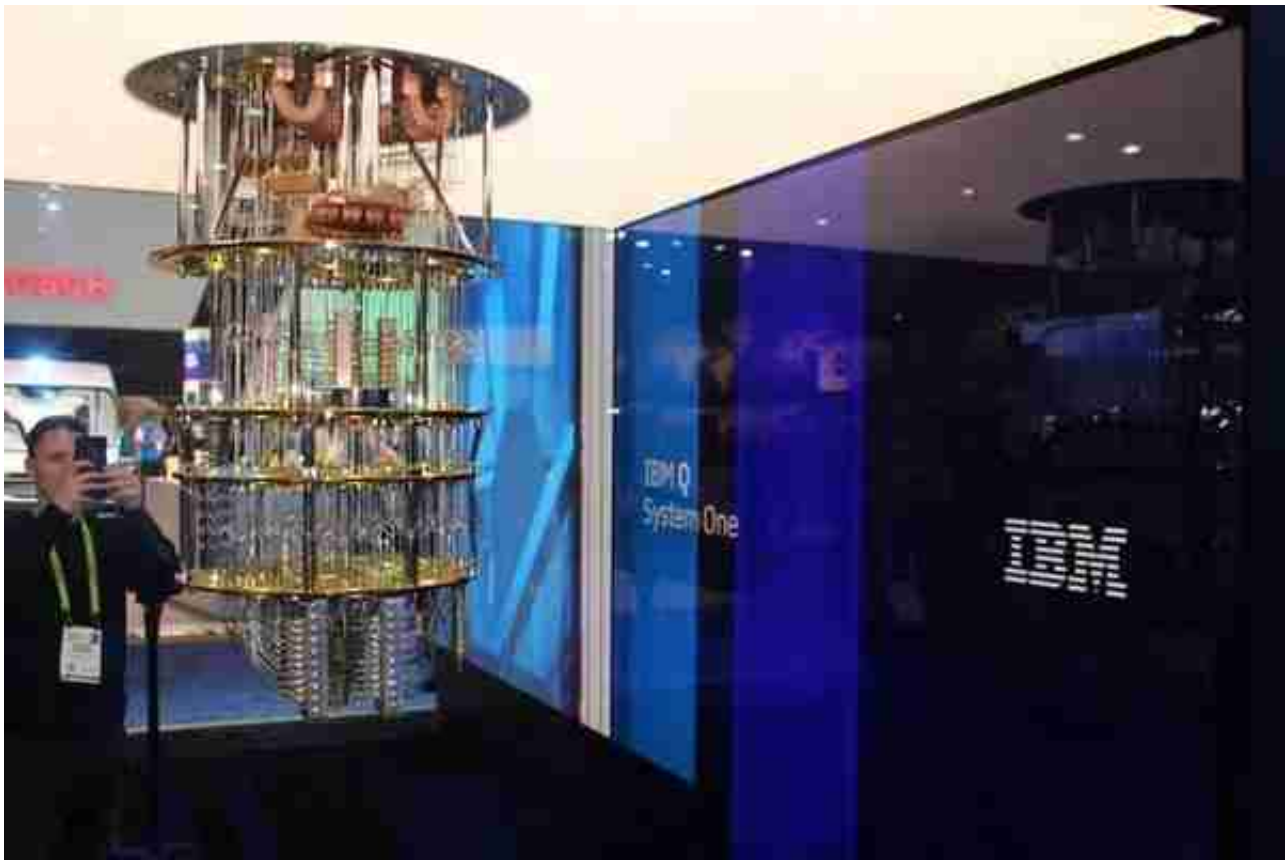
比特币的安全协议使用了两种加密算法，即挖矿过程中使用的哈希算法和在区块链上提供数字签名的非对称加密算法。新加坡国立大学的研究人员认为十年后量子计算机的算力和挖矿速度会飞速增长，量子计算机能很快破解哈希函数，从而垄断整个区块链，让比特币的安全协议作废。

除了通过强大的算力进行51%攻击外，量子计算机更大的威胁在于加密货币使用的非对称加密算法。大部分专家认为量子计算机可以轻松破解目前加密货币使用的椭圆曲线数字签名算法，从而通过逆向工程从公钥推算出用户的私钥，如果真的出现这种情况，会对加密货币造成毁灭性打击。专家预测到2027年量子计算机的舒尔算法能在十分钟内破解密钥，Lund表示目前公布的区块链项目中至少有一半可能会受到影响。

“从公钥逆向推算私钥意味着获得钱包的管理权限，私钥本质上就是加密货币钱包，比特币是一个公开的账本，也就是说，其他人可以得知哪个地址持有大量比特币，攻击者可以把持币多的地址作为目标，我认为这是非常大的威胁。”

由于量子计算机几乎威胁到现存的所有加密系统，如“通信、银行、个人设备、政府数据库”，IBM团队认为，包括比特币和以太坊在内，几乎所有的虚拟货币都必

须采取预防措施来减轻和预防量子计算机带来的威胁。IBM数据安全服务公司首席技术官Nev Zunic表示，加密货币的技术负责人应该从现在开始采取应对“量子计算机威胁”的措施。在瑞士“IBM Research”中担任安全性及隐私集团经理的Michael Osborne警告说，由于量子计算机的发展将在虚拟货币安全上设置了“时限”，所以在事态严重化之前，必须采取相应的计划。



Nev Zunic表示，量子计算机可能需要10年或更长时间的发展才能对我们造成实质性威胁，但他补充说：“我们现在发送的加密数据也可能会受到量子计算机的影响。现在进行的加密通信有可能被监听和保存下来，并在以后被量子计算机破解。”

也就是说，在政府机关、军队、金融交易等机构进行高机密性的通信的情况下，这些数据也有被监听、保存之后破解的风险。为此，相关机构为了避免出现此类的风险，必须从现在开始采取相关行动。

量子计算机也是这几年才被社会广泛得知，不过几乎没有多少普通人可以理解它的具体结构和功能。但是，理解这些技术的专家们从很早以前开始就对“量子计算机所带来的威胁”持续发出警告，许多人建议尽快采取应对措施。目前虽然存在一些号称能够抵御量子攻击的虚拟货币，但从已经发行的虚拟货币整体情况来看，具备这种耐性的货币所占比例非常小。

然而，量子计算机的实用化正在稳步推进，IBM发布的“IBM Q System One”只是一个开始，认识到量子计算机意义的各国政府和大型企业都在加大相关研发力度，量子计算机的计算能力正以每年翻一番的速度飞快前进。量子计算机的发展是毋庸置疑的，它终有一天将会威胁到区块链，但似乎区块链的很多专家们还没有警惕起来，甚至将抵御量子攻击的希望放在其他大型组织上。在他们看来政府和传统金融机构面临的风险更大，和新兴的区块链行业相比，这些组织的技术实力更加强大，会在受到威胁之前推出相关的解决措施。

很多相关机构正在研发足以抵抗量子攻击的量子密码系统，如果成功的话或许量子计算机的威胁永远不会到来，但对于完全建立在加密算法和共识机制之上的区块链技术而言，没有作为显然会对其信任系统造成打击。对那些与虚拟货币相关的人士来说，从现在开始好好地面对这些威胁是非常重要的。