近几年来，量子计算发展迅速。前不久，谷歌宣布实现量子霸权，我国“天河二号”超级计算机计算出量子霸权标准。所谓量子霸权是指，如果能证明量子计算机在某个问题上计算能力远远超过目前性能最好的超级计算机，就实现了量子计算机对传统计算机的霸权。量子计算的发展极大挑战了现有密码体制，理论上量子算法能破译Diffie-Hellman算法、RSA算法、椭圆曲线算法等非对称密码算法。

由于密码学是区块链的关键要素，是实现数字货币安全可信的技术基础，因此人们不免担忧，量子计算的发展是否会对区块链和数字货币的安全带来威胁，甚者有人断言在量子计算机面前，区块链不值一提。但目前看，定论尚早。一是量子计算算法（如Grover算法和Shor算法）对非对称密码体系的威胁较大，但对对称密码、哈希算法的影响相对较小。二是目前没有证据证实或证伪量子计算机可以解决NP（Nondeterministic Polynomial，非确定性多项式）完全问题，也无法轻易地论断在量子计算环境下，依据计算复杂性的密码技术就没有前途了。三是密码学历来是在编码和破译、攻击和防守、矛和盾的对抗中发展起来，不能说有量子计算了，密码就不行了，量子计算也有其不擅长的地方，亦可构造抗量子密码体制，比如多变量公钥密码体制、基于Hash函数的数字签名方案、基于纠错码的密码体制和基于格的密码体制等。

因此，量子计算是否让区块链和数字货币失去了发展意义，短期内并不好说。但有一点是肯定的，那就是随着技术的发展，货币形态以及货币技术必然也会发生相应的改变。在量子时代，基于区块链技术的加密货币或许将继续存在，只不过它可能会采用更先进的抗量子密码技术。而另外一种可能是，它将被一种新型的基于量子技术的货币形态替代，也就是现在学术界有人在探索的量子货币。

量子货币的概念

量子货币本质上是一种基于密码学的数字货币，其优于经典数字货币的核心是利用量子叠加态和量子计算而实现的量子防伪技术。这项技术综合运用了物理学、计算机科学和密码学等多个学科领域的前沿知识，最终可在不引入记账机制的前提下解决货币双花问题。理想的量子货币可同时实现易于识别、难于伪造、无法复制、方便使用等数字货币特性，同时结合了传统货币（纸币）和经典数字货币的优点，并避免它们各自在本质上难以克服的缺点。

1969年美国哥伦比亚大学研究生Stephen Wiesner首次提出量子货币的概念，他设想在货币上配备一个储存光子的量子器件，利用量子态作为货币的防伪标识，但只有发行货币的中央银行才能检验货币的真伪。1982年，Bennett等人试图建立第一个公钥量子货币。他们的方案仅允许一张货币花费一次，将其称为“地铁通行证”。后来人们发现他们的设计存在两个不安全因素：一是基于不明传递的不安全协

议；二是可被Shor算法破解。2003年，Tokunaga等人改进了Weisner的方案，不必要求中央银行追踪每一个发行的货币，而是采用特殊的方法保证货币被修改后依然有效，这允许货币持有人在银行验钞之前对货币进行修改，实现货币交易，但缺点是，银行一旦发现*****必须立即发布信息，清除*****之前的全部交易信息，因此该方案不易实现。2009年，Aaronson提出复杂理论不可克隆定理，假设存在一个机制可以验证给定态是否等于一个有效量子货币态，一个伪造货币者如果想伪造货币必须同时拥有该验证机制。2010年，Mosca和Stebila指出一个货币伪造者即使拥有一个量子货币验证机制，也仍然不能制造出比他初始状态更多的量子货币。授权商运行一个模糊验证方法，在得到最终结果之前得不到任何有用信息，在验证过程中他必须与银行进行通信，该方案是一个量子货币私钥方案。2012年，Lutomirski等人利用扭结不变量的方法提出了一个真正意义上的量子货币公钥方案。但是，该方案的安全性目前还没有人能够证明。2015年，Subhayan等人提出量子支票协议，该协议中可信银行的任何一个合法客户端都持有一个“量子支票书”，可以发行支票，并与银行之间共享一个经典信道，由银行或它的分支机构完成货币验证。

量子货币的基本原理

量子比特、量子叠加态

在经典计算机中，比特“0”和“1”都是用经典物理量编码表示的，例如可以用电压、磁场方向等，而经典物理量测量结果是唯一确定的，即一个经典比特不可能同时处于两个状态（比如同时处于“高电压”和“低电压”状态）。而量子比特是基于微观粒子的量子态存储的，其不同于经典物理状态的最重要的特点在于可以同时处于若干个微观量子态的叠加态。例如用|0>表示一个电子的基态或自旋向下，用|1>表示激发态或自旋向上，则一个微观量子态可以表示成|>=a|0>+b|0>，其中a，b都是复数，且它们的模长平方和为1。图1显示了经典数据位与量子数据位对比图，经典数据位的表示要么是0，要么是1，而量子数据位是|0>和|1>的叠加态，即可以是0也可以是1。