姚前：量子货币：一种学术假想 | 互联网金融

文/时任中国证券登记结算有限责任公司总经理，前央行数字货币研究所所长姚前

本文认为，量子计算是否让区块链和数字货币失去了发展意义，短期内并无定论。但随着技术的发展，货币形态以及货币技术必然也会发生相应的改变。在未来的量子时代，量子货币或将登上历史舞台。本文剖析了量子货币的概念、缘起、逻辑和基本原理，指出量子货币的核心问题及研究方向。虽然量子货币理论还存在瑕疵，但值得我们关注与探索。

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，银行一旦发现伪钞必须立即发布信息，清除伪钞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。

理解量子货币的逻辑出发点：**伪造与双花****

货币发展史是防伪技术的发展史，也是生产者与伪造者不断斗争的历史。不管是贝壳、金属、纸、塑料还是电子的货币形态，防止伪造都是货币生产的最重要目标。尤其是到了信用货币时期，货币本身的价值属性逐渐弱化，货币防伪显得尤为重要。可以说，不能防止伪造就谈不上货币。然而，历史上从来没有一种货币可以完全解决被伪造问题，货币伪造史与货币发展史几乎一样长。直到现在，人民币、美元和欧元等各国纸币伪造案例仍时有发生。

传统货币伪造屡禁不止的一个根本原因是经典物理的易伪造特征。按照经典物理的基本原理，物理状态都可以被精确测量，只要能按照测量结果，以足够应对检验的精度重新组织物质，就可以达到伪造货币的目的。传统的货币生产机构研发的各种防伪技术，例如金属货币的花纹、锯齿，纸钞的水印、安全线、纤维、光变油墨、胶凹印特征等防伪特征，本质上只是在抬高伪造货币的门槛，但不能从根本上禁绝。虽然说可以让伪造的成本足够高以至于伪造货币无利可图，从而避免伪造，但随着技术的不断发展以及高精尖技术向民用领域的广泛应用，伪造的技术门槛亦可能下降。若伪造者投入足够物力、财力和智力，任何传统货币防伪技术在理论上都有可能被破解。

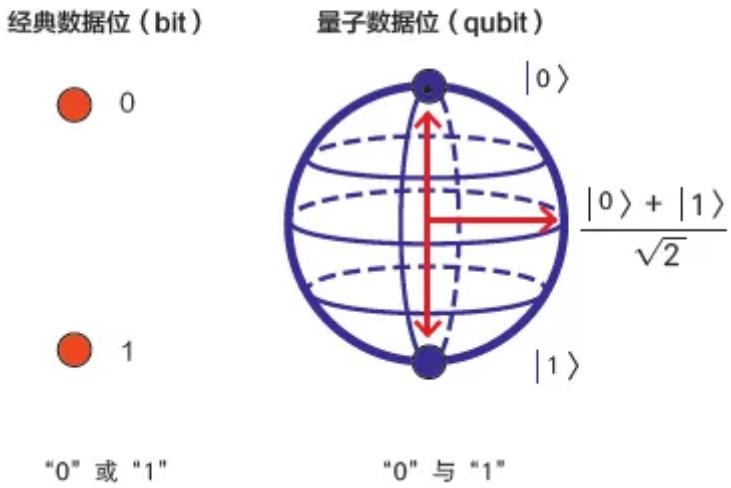
对于电子货币和数字货币而言，其形式上就是一串二进制的信息，它们需要解决的问题比纸钞的防伪更加麻烦，因为在计算机里信息很容易被复制。这串信息可以利用密码学技术来防止伪造。比如说数字货币的发行机构可以对发行的每个数字货币进行签名，这样每个人都可以很方便地验证货币的真伪。此外，数字货币还存在双花问题。在甲方和乙方的交易中，如果没有任何其他人知道，甲方完全可以在和乙方交易之前偷偷备份相同的数字货币，然后假装和乙方的交易没有发生，与丙方进行交易。解决的方案是采用一个账本的形式来记录已经发生的交易，以此避免同一笔数字货币被多次花费。这个账本既可以是银行或者支付宝那样的中心化账本，也可以像比特币一样采用基于区块链技术的分布式账本。量子货币则通过量子不可克隆原理来解决货币的伪造和双花问题。

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。

图1 经典数据位与量子数据位对比图



量子货币如何防伪防双花

微观量子态本身含有的信息非常丰富，但我们只能通过测量的方式获得其信息，而测量的行为反过来又会影响量子态，造成被测量的量子态坍缩，最终每个量子比特测量后仅能得到一个关于坍缩到的量子态的信息。另一方面，量子世界中，克隆是不可能的。换句话说，并不存在任何一个电路，能做到这样的一个功能：输入是任意一个未知的量子态，输出是两个该量子态。此为量子不可克隆（复制）基本原理。

量子不可克隆原理构成了量子货币的理论基础。量子货币在本质上也是一串信息，这点与电子货币和数字货币类似，但不同之处在于，量子货币除了经典的二进制编码信息外，还包含以量子比特的形式存储的量子信息。采用量子比特的好处在于每个量子比特都能以叠加态的形式保存远比经典比特丰富的信息，并且这些信息无法被精确测量出来。根据量子不可克隆原理，对量子比特的测量都必然导致量子态坍缩到其中某一个叠加态上，从而永久地损失掉所有关于其他未坍缩到的状态的信息。这样就可以在本质上防止量子货币的信息被测量和复制，因为量子物理学保证了对量子比特的测量无法获得完整的信息。此外，量子货币还可采用与数字货币相似的密码学技术，避免被攻击者伪造。

量子不可克隆定理还可防止量子货币双花。具体来说，量子货币拥有者只能拥有量子态，但不能知道每一个量子态是什么，他若想知道，只能测量，但一旦测量，量子态则会塌缩变成另一个量子态(原来叠加态中的某一个)，相当于量子货币拥有者自己把自己的货币销毁掉了。这样“持有量子态但并不知道量子态”的设计有效防止了货币双花，因为如果量子货币拥有者知道自己手里的量子态是什么的话，他其实是可以“克隆”很多份。

量子货币的点对点支付

相对于传统货币，数字货币的最大优点就是在于传输方便，仅需要通过网络传输信息，而不需像传统货币那样传递实物。量子货币也一样，只需要传递量子态所包含的信息即可。传递的量子态信息既可以通过发送包含这些信息的粒子（比如光子）实现，也可以通过量子通信在经典信道实现——即通信双方事先分享一个纠缠的量子态，然后仅通过经典信道传输经典的二进制信息就可以实现传递复杂的量子态的任务。

因此，基于量子货币的交易可以在交易方之间直接进行（至多只需要一个可信的第三方事先分发纠缠的量子态），不需要通过第三方账本验证。

量子货币的核心问题：如何验钞**

虽然“持有量子态但并不知道量子态”使我们能利用量子不可克隆定理解决量子货币的双花问题，但同时也带来了新的问题，即如何验钞。在甲方付款给乙方的交易中，既然乙方不知道自己持有的量子态的信息，且无法通过测量得到足够的信息，那么他如何确认这是一枚合法的量子货币，不是甲方随意制造的或者是甲方已经观测过的？而如果允许采用测量的方式来验证量子货币是否合法，则甲方可以先测量自己的量子货币的量子态，然后按照坍缩后的状态构造新的量子态再发送给乙方。因为甲方知道坍缩后状态的所有信息，他可以再重新构造一个坍缩后的量子态发给丙方，这就引发了双花问题。因此，乙方无法判断甲方是否花费过这一枚量子货币，而且也无法判断坍缩状态是自己观察导致的还是甲方的观察导致的。

在理论上，无损的量子货币验钞是可行的。量子叠加态的坍缩是在有多个叠加态的时候才会发生，而如果只有唯一一个状态，就不会发生坍缩。因此，可选择“适当的”变换，使每一个合法的量子货币的量子态在经过该变换后都会在“适当的”量子比特位置上呈现出不会坍缩的唯一状态，然后再部分地测量这些量子比特的状态，不测量其他处于叠加态的量子比特，如此可在不损害原有量子态的情况下获得量子态的信息。而且如果原来的量子态是通过“适当的”密码学签名编码构造的，则这些测量出的信息就可验证原量子态编码的量子货币的合法性。

一个理论上可用的量子货币方案必须在上述的三个“适当的”地方都做出正确的选择，并给出数学上的证明。除了实现无损验钞的功能以外，还必须确保不存在验钞程序漏洞。解决这些问题，需要充分发挥密码学的作用并与量子计算相结合，探索量子加密手段，使量子货币的检验达到物理意义上的安全。

关于量子货币验钞机制的研究问题还包括：验钞是否可脱离中央银行，由持币人独立完成检验/验钞过程是否会给量子态带来损耗？是否能支持多次验钞？损耗是否会导致一定概率出错？如何应对噪音？

结语

科学总是在假想的证实和证伪中不断发展，这或许就是假想的价值。“在量子计算机面前，区块链不值一提”当然也是一种假想。从某种意义上来说，提出问题比解决问题更重要。数字货币的假想可追溯至20世纪70年代以来密码学界的梦想：手里的现金能不能像邮件一样，加个数字信封，进行加密和签名后，从一端发送到另外一端。这一梦想在大卫·乔姆、中本聪等人的不懈探索下，逐步发展为席卷全球的数字货币试验。历史表明，货币形态演化和内涵扩展受到了历次科技进步的深刻影响，这一进程不会在量子时代就此终止，而是不断向前发展。当前量子技术还支持不了量子货币，量子货币理论也存在瑕疵，有学者甚至认为未来是否适用尚难断言。但量子计算正加速发展，量子时代已不再遥远，正向我们趋近。新技术带来的挑战和机遇，值得我们关注与探索。