# 第10讲 量子计算与区块链

量子力学，很多人冠以“怪异”的形容，因为其本生的不确定性和纠缠等性质，和我们日常生活的世界，似乎格格不入。但是，随着基于量子理论的半导体工业把人类带进了信息网络时代，人们发现完全无法忽视量子世界认知的意义。随着现在量子理论和实验研究的不断深入，尤其是量子通信、量子计算的发展，让人们终于开始认识到当初似乎对立的玻尔、海森伯的哥本哈根学派和爱因斯坦的量子世界“非定域”认知，正在殊途同归。人类开始认识到之所以量子力学表述初看起来“怪异”，实际上是自牛顿起，整个经典物理学接受了源自希腊“原子论”的定域决定论，而以科学的名义放弃了早在《道德经》、《圣经》、《金刚经》中大量出现的宇宙“非定域性”的智慧描述。

量子力学、量子通信、量子计算等最新的发展，逐渐昭示人类：人类文明从不同路径，不同时空，正在走向一个同样的顶点！

利用量子特性（如非定域性不可克隆原理），结合区块链技术，新的量子货币设想由此诞生。

### 10.1量子本性与量子计算

**波粒二象性是量子力学的本质吗？**

经常一本量子力学教科书，一开始都会从波粒二象性展开陈述。如果坚持波粒二象性，量子力学就不能自洽了，因为“波”和“粒子”本身就是两个相对、不能互相转换的概念，非要把它们放在一起，本身就不合理。

 费曼在《费曼物理学讲义》说了，单电子双缝干涉实验奠定了量子力学的基础，理解这个实验就理解了量子力学的一半。

前面第一讲的1.5中我们介绍过单电子双缝干涉实验，是日本物理学家殿村教授实现的，我们只能得出一个结论：一个电子在同时走这两个缝，电子自己和自己发生了干涉【12】。

 这从表面上看与我们平时接触的常识相对立。前不久清华大学顾学雍教授给我推荐了BBC的纪录片【2】，里面讲述了生物学上的光合作用，生物学家也百思不得其解，最后只有通过量子力学的非定域性才得到合理的解释。所谓光合作用就是细胞中有一个量子在接受到光以后，把能量传递给别的细胞，量子如果是定域的，也就意味着量子必须走固定路线去进行能量的传递，那么要完成光合作用需要花1000年的时间，这和现实观察严重不符。因此光合作用只能从量子的非定域性去解释。

因此，我现在不用“波粒二像性”这个词，我用“非定域性”，我认为是更本质的解释。很多词都是一种误导，刚刚那个现象也无法用波粒二象性进行解释。我们目前可以得出的初步结论是：电子是非定域的，不确定地存在于时空的哪个点上。

**坦率来说，牛顿和爱因斯坦最早强调的“原子”“定域因果性”，让我们相信“眼见为实”，我们只相信我们所看到的，这一点极大限制了人类的思维，但量子力学帮我们揭开了一个帷幕：看见的信息后面，还有一部分万物关联，看不见的东西并不是不存在，这解释了很多传统视角下不可思议的现象。**

所以我认为“波粒二像性”应该更本质的表述成量子二象性：“整体的非定域关联和定域的信息”，两者之和才构成了一个完整的世界。看不见的世界是关联性的，就跟刚刚提及的单电子双缝实验，单电子同时经过两个缝的路径是彼此关联的，当然你可以通过测量得到定域方面的信息，但你看见的绝对不是世界的全部。

**不确定性原理的后面就是不可知论吗？**

很多人说不确定性有两派争论：一派是爱因斯坦，他认为量子学的不确定性和热力学的不确定性是一种性质，热力学的观点是“随机性不是事物的本质”，它们背后还是遵循定域确定性的牛顿定域，之所以出现随机性是因为自由度太多了，比如说在我们今天所在的这个讲堂上，有十的几十次方个分子，你要精确地知道每个分子的信息轨道，信息量太大，几乎不可能，只好退而求其次的用统计性的“粗粒”描述。热力学基本是这么一种思考方式，是非常能自洽的一个理论。爱因斯坦认为，量子力学后面也有这种定域确定性的定域，只是我们现在还没看到。

 一派是玻尔和海森伯，他们非常坚持“量子的本质就是不确定性”，他们的代表性观点就是波粒二象性和海森伯的不确定原理。

两方在这一点产生了剧烈的争论，最后就归结到了量子纠缠。因为不确定性非常直接地产生量子纠缠的现象。以自旋来说，量子天然存在不确定性，量子自旋态应该是向上、向下是同时叠加的，但是两个电子角动量守恒的话（假设初始角动量为零），这两个东西很容易产生矛盾：

第一章1.5我们已经论述了量子纠缠产生的必然性，而且两个电子分得再远也是纠缠的，但这个是我们生活中我们很难想象的。因此量子纠缠让爱因斯坦很难接受，因为相对论理论的基石是任何物体的相互影响不能超过光速，但纠缠似乎暗示量子的关联是瞬间的，因此他后来提出了EPR悖论。

 爱因斯坦和玻尔争论很激烈，刚开始很大程度上是哲学的争论，后来通过物理实验，让贝尔不等式与实验去对照，去判断纠缠是否存在。1982年相隔瑞士的日内瓦湖十八公里的两个实验点证明：量子纠缠确定存在，量子理论无法和经典的定域概念兼容。这个试验被物理学界主流所接受。【4】

很多科普文章因此都说爱因斯坦被玻尔他们彻底打败了，我后来在张礼先生指导下查了很多文献，看到1933年爱因斯坦在牛津大学演讲时说：“我们必须放弃粒子在理论模型中完全定域的概念，我认为是海森伯测不准原理的永久性结果。”【5】他能说到这一层，我认为他不愧是超越时代的大师。因为他提出了量子力学最本质的东西：非定域性，这句话为量子力学未来能够架构出了一个真正能理解的自洽世界奠定了基石。

不确定性只是表象，真正的本质是“非定域性”。我们看到的世界只是得到整体世界信息的一部分，而后面的世界非定域关联，你还没有看到。

 我觉得恰恰是爱因斯坦真正把海森伯“不确定性原理”的本质一下点破了。爱因斯坦追求一个世界一定是完美自洽的，虽然玻尔他们提出了理论，也得到了实验的验证，但后者的整个认知体系一直没办法自洽。

 那么量子的非定域性和不确定性究竟是什么关系？我想到了一个中国成语：**管中窥豹。**

人受时空限制，你每次观察和看到的，都是定域信息，就像用一根细管去看一个整体的豹，因此你看到的是随机的，要么看到黄的，要么看到黑的，但你看多了，拿大数据分析，慢慢你发现它们是有关联的，注意，大数据里特别重要的就是发现了“非因果性关联”。实际上，量子力学让大家真正认识到万物关联是一个整体，这才是我们时代最大的认知特点。

 当然从表面上看，量子是具有不确定性的，但并不是不可知论。有人一知半解的说量子力学的不确定性意味着“月亮你不看它就不存在”，这是荒谬的。所谓不确定性，是因为人观察世界总有定域局限性，不确定性是背后整体关联的反映，量子力学的巧妙之处并不是告诉你不确定性，而是人类第一次用科学去描述后面的整体性关联，可以精确计算，用实验对照去做科学的结论。先哲圣人是鹰，可以说直接飞到山顶，而量子力学是找到了路径，一个常人可以使用的科学方法去攀登到那个山顶。

 总结一下，玻尔和爱因斯坦之争，现在看来各有所长，玻尔他们发现了波粒二象性和量子力学方程，但真正的哲学概念以及本质还是爱因斯坦发现的，他们两之争很难说谁输谁赢。

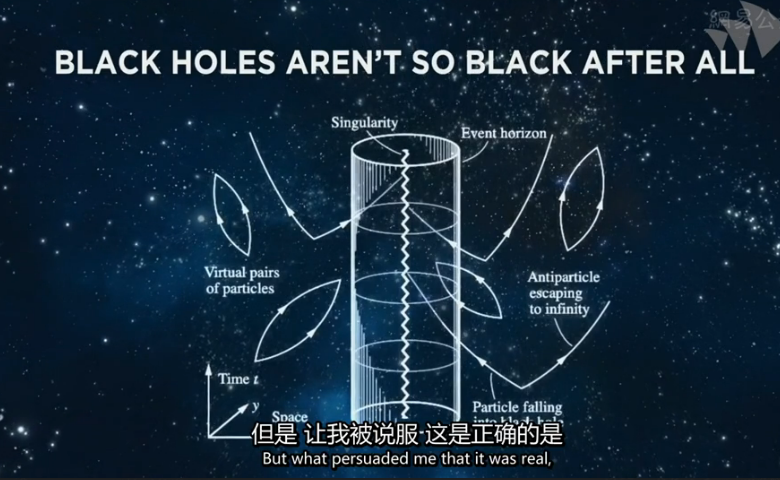
**薛定谔猫是最诡异的吗？**

猫死猫活怎么能同时存在并纠缠在一起？这件事看起来本身就很怪异。费曼提出观点：**一个量子的过程，如果有两个以上的路径选择，一旦决定选择采用了其中某个选择，就破坏了两个路径的关联。【6】**这实际上也就是第一讲1.5所表述的Englert-Greenberg-Yasin关系（定域度一旦为一，量子关联度将为零）。以这个角度看，薛定谔的猫就不难理解，因为猫死或者猫活的信息我们是一眼就能识别的，所以他们之间就算有量子关联也会马上消失（退相干），我们在现实生活中是不可能观察到猫死和猫活同时叠加的量子状态的。  
  
那人类怎么得到这个定域的信息呢？第一次从数学角度去解决这个事情的是计算机之父冯·诺依曼，他提出了获得量子定域信息的方法，获得信息首先要把一部分量子和环境的纠缠切断（退相干），即可以获得这部分量子的定域信息。【9】

假设薛定谔猫成立，猫死猫活与原子衰变纠缠了起来，但是猫死猫活是我们一眼就可以得到的信息，或者说因为猫本身太大，是宏观物体，它与空气中无数分子纠缠，我们很容易切断关联。在现实世界很难看到这种量子纠缠现象，并不是因为它不会纠缠，而是它极快就退相干了。

 有个人因此下了一个结论，做任何物理实验一定要有人观察，去截断量子关联，不然我们没法得到信息，这个理论表面看起来并没有问题，但是有人又把这个结论推到极端，写下诸如此类的标题：“假如我们不去看，月亮就不存在”。我曾经也有这个困惑，直到我听到了霍金的黑体辐射理论。

 大家知道，黑洞有一个视界，也就是眼睛的极限，视界之内，因为引力太大，光都出不去，我们没办法探测黑洞里的任何信息。因为黑洞引力太大，根据量子的不确定性，真空会被撕裂成正电子、负电子，产生的时候一定纠缠（保持自旋等物理量守恒）。如果这样，正好正电子被拉进黑洞去了，负电子辐射出来。霍金受这件事启发，最终想出了一个解释，纠缠的量子在分开之后还是纠缠状态，还是符合能量和自旋守恒定域，这样的纠缠天然被黑洞视界截断了，这就是霍金最巨大的贡献，黑洞不是纯黑的，是不断往外辐射物质的，辐射出来的物质与黑洞里面物质的纠缠被黑洞视界截断，这就是我们看到的定域世界信息。



**（由**2015年4月26日**霍金在澳大利亚演讲时截屏展示：黑洞视界用二维圆圈表示，柱体表示圆圈视界随时间向上形成时空曲面，周围带箭头的开或闭合的线都表示黑洞引力造成的真空撕裂（涨落），闭合的线代表自生自灭的需电子对产生过程，一端闭合一端开放表示正电子被拉进了黑洞，与之纠缠的负电子形成了“霍金辐射”，由于正负电子对的量子纠缠正好被黑洞截断，根据冯\*诺依曼理论，负电子释放了我们看到宇宙的定域信息。）**

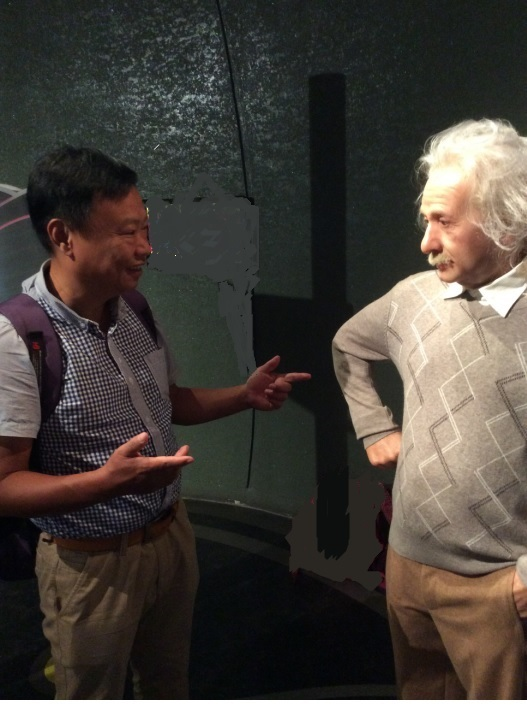
因此，量子力学一点都不怪异，是人类智慧的某种力量的结合，它并没有产生奇形怪状的东西，它有科学的依据和方法路径，通过这个路径，谁都可以走入这条路，同时它也不断为人类提供新的知识。按这样来说，所谓不确定性只是我们看到的世界的一个方面，但是世界是一个整体关联，每个人得到的信息是定域的，但对于整体关联，它是可以通过量子计算以及实验大数据去认知的。

**我们的世界是一个整体性关联的存在，我们所谓的不确定性，只是我们人类观测本身时空定域限制的结果。**

**爱因斯坦真正被量子纠缠打败了吗？**

实际上，不是这么回事，让我们具体来看看量子纠缠在量子通信上的应用。

量子通信是最安全的系统，因为量子秘钥的瞬间传输利用的就是量子纠缠，如果有窃听的话，它会马上“塌缩”，对方可以立即停止使用该秘钥。因此理论上，量子信道是绝对安全的。所谓量子隐形传输是技术上可以做到瞬间把量子态传递到无穷远，但它并不违背爱因斯坦光速不变的原理。相对论的出发点是任何经典信息传递不超过光速。经典信息是定域的，而量子态我们前面说了是非定域的，因此瞬间传递量子态并不是传递经典信息，传递信息还是需要通过经典的通讯通道，这个不能超光速。因此爱因斯坦的相对性原理，到今天为止没有被实验否定。



**在上海杜莎夫人蜡像馆拍的这张像，表达我对爱因斯坦永远的崇敬**

总结一下，量子力学发现的是一种关联，代表世界最基本的整体性，在某些条件上能转换成定域的信息，但后面的整体性还是存在的，所谓的薛定谔猫是退相干，关联被切断了；量子纠缠与光速不变原理绝对不矛盾，量子态可以瞬间传递但不是传递定域信息，三体中的超光速传递信息不可能；很多人嘴里爱挂着平行宇宙，但实际上平行的是量子的非定域性，如果你真活在一个定域的世界中，那个关联早就被切断了，你没有同时活在两个以上定域世界的可能，那样的话首先能量守恒就已经被违反了。

**从量子非定域性到量子计算**

有了量子力学这两个基本点，一个是非定域性，一个是纠缠，这个量子计算就很自然的产生。

量子计算就是利用所谓的并行性（parallelism），根源就在于量子非定域性。如果你真正理解了量子非定域性，你马上就理解量子计算的强大，因为它的这种非定域性同时存在好多 态，这是天然 的，TA只要不被破坏的话，他可以同步进行计算很多步。

但是曾经有一个清华的计算机专业的朋友来问我，说不对，你这个事情并不会节省经典计算的步数，因为你最后要测量，你如果一个态一个态的去测量 ，因为一个经典的计算得到的是一个比特最后的确定性，量子计算是非定域的运算过程，结果也是非定域的，你怎么样得到定域的结果呢？如果你靠一步一步的测量 的话，那一样的，麦克斯韦妖最后在最后测量中也一样耗散能量，实际上并没有节省什么。

经典的思路当然的一步一步去算，你没有其它更好的办法，但是实际上我们面临的大量的数据x问题，并不需要知道f(x)本身确定的值，我只需要知道你f(0)和f(1)之间这两个运算结果相等或者是不相等，大数据基本上属于这一类。大数据并不要求大数据处理要你每个数带进去一个函数都算出来，你希望得到大数据所谓征信数据，基本上我们只要抓住大数据的整体特征，要么相等要么不相等，基本的征信结论可能就出来了。

你明白这个以后，量子计算就派上用场，比如说我只需要知道这个函数零和一带进去，更多 的数也一样，他们要么是相等，要么是不等的，我只需要这个结果，那么Deutsch量子算法怎么做？【17】



很简单，利用量子非定域性，如上面（1）先叠加x，一定要利用量子叠加，x可以很多个量子比特同时叠加，你原来只有一步一步算的，你现在可以把上百万的x同时往里代，（1）后面的量子态y是操作态。操作态就是说在量子计算下，操作态操作成y+f(x)，如果f(x)等于零的话，这个将不翻转，如果f(x)等于一的话将翻转(因为二进位制)。

为什么f（x）是1就翻转？这是二进位，如果Y是0的话，这边是1，y加1等于1，已经翻转了，最后结果是1，如果你x=1的话，这边f（x）=1，一加一等于二，但是对于二进位比特来讲，他必须进位，所以就变成了0。

所以就意味着f（x）=1，后面的量子比特y就会翻转，一翻转最后得到的一个态是纠缠态.更巧妙 的是，Deutsch把后面的这个所谓的操作态y设计成如（2）式。你把前面的x代进去，前面是0+1态，当然他用量子的非定域性，通过量子计算，你很容易得到。那么对于后面操作态y来讲，如果f(1)不等于f（0），因为如果f（1）=1会造成翻转，而f（0）=0不翻转，所以输入1让后面操作态（0-1态）一翻转就会带来一个负号，这样就给前面的态施加了一个标记。

当f（0） 不等于f（1），就是输入0和1的结果有区别的时候，后面第二个量子比特将翻转，这就出现一个负号，最后你只测量 一步，你就能得到结果了.本来经典计算必须算两步，你必须算一个f(0)和f(1)，但是量子的计算只要一步就出来结果。

这种量子算法 ，不要看就这么简单的一步，当你的x是非常巨大的数的时候，就有巨大的优势，因为你量子非定域叠加是没有限制的。

现在大数据，谷歌现在非常积极的尝试运用量子算法，据说他们找到了处理大数据的量子算法。

据说在阿里巴巴每个用户，每天给他贡献的大数据都是100M，按经典，用云计算去处理都是一个受不了的事情，但是用量子计算，100M可能一步就完成了，他就把你的特征能够提取出来。

下面介绍一个大数质数分解的Shor量子算法。

一个大数，比如：**1522605027922533360535618378132637429718068114961380688657908494580122963258952897654000350692006139**

把它进行质数分解：**37975227936943673922808872755445627854565536638199**

**×40094690950920881030683735292761468389214899724061（由孙晓明博士提供）**

这样的问题因为正向运算很难，而反向验证很容易，所以是加密算法RSA-100的基础。

而Shor给出了一个成功的量子算法。

经典是怎么算的呢？

**Classical part**

* Pick a random ***a*∈{2, 3,…, *N*-1}**
* Let ***f* (*x*) = *ax* (mod *N*)**, use **period-finding** to find period ***r*** of  ***f* (*x*)**, i.e.

***ax+r* ≡ *ax* (mod *N*).**

* If **2|*r***, compute **gcd(*ar*/2-1, *N*)** and **gcd(*ar*/2+1, *N*)-------（3）**

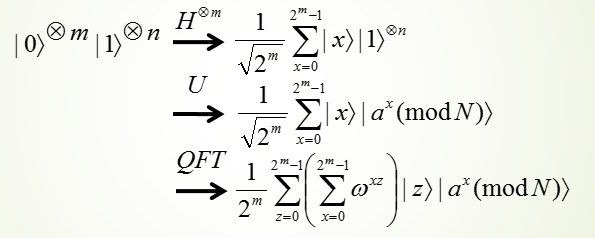
**（孙晓明博士提供）**

上式（3）中假定这个数是N，我取a，a是2到N—1任何一个数，我们算它的x次方对N的余数，定义f(x)是它的余数。

我的目的是要找到周期的规律，如果你能发现一个a在(x+r)次方的余数，正好等于a的x次方的余数（对于N），而r又是2的倍数，你就找到一个周期率，有了这个周期率以后你就能质数分解了，如（3）式，那么**(*ar*/2-1, *N*)**他们之间的最大公约数跟这个**(*ar*/2+1, *N*)的**最大公约数 ，正好就是N分解出的质数。（得到这个结论需要一个数论定理，在此不赘述）。

所以经典的算法很简单粗暴，你就不断的取a把x往里带，你碰到周期性就有效，跟比特币挖矿差不多，基本上随机碰撞。所以传统的经典的办法，就是把N取到足够大，让你的算力需要大到一般计算机完全对他无能为力，就算加密成功了。

量子算法怎么办？

----------(4)

（孙晓明博士提供）

如（4）式，开始量子态是0，对于它我们可以做Hadamard变换，这样可以利用量子非定域性让很多x同时参与运算，（4）式中第二个量子比特是操作态，操作自然就是对N求a的x次方的余数，跟经典的一样。但是我们操作这些，我们的目的是非常快的找到那个周期率，用的是一个量子非定域态很多x同时计算，如果提前输入的诸多x有符合这个周期率的话，通过后面的QFT变换是可以测量出来的。

下面说一下量子搜索算法（Grover算法）：



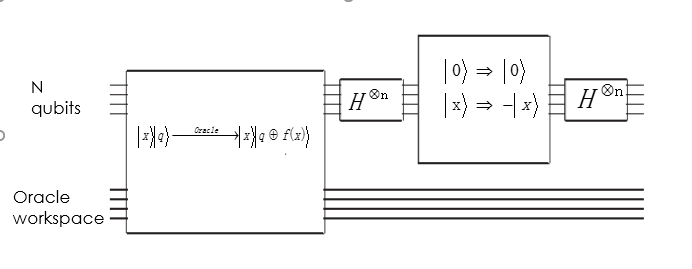
（5）式中给出的量子搜索的算法【17】， 核心思想就是做标记Oracle。所谓搜索也很简单，我们面对一个很大的数据源，搜索就是如果找到的x符合标准，比如说我在北京城市里上千万人口，我们要找到小明是谁，符合我这个标准的，那就是f（x）=1，其它不符合都是f（x）=0.那如果经典算法的话，你只有一个一个去算，别无他法，你把这几千万数据挨个带进去。

但是所谓量子搜索他怎么干？他的设计跟前面很相似，（5）就是根据量子非定域性设计一个态，理论上可以把很多x同时叠加输入，（6）式中的第二个量子比特q是操作态，当f（x）=1的时候q态就翻转（也就是找到目标），f（x）=0的时候就不翻转。（7）式中Grover把操作态设计成0-1态，它就起到做标记的作用，当f（x）=1的时候，你把上百万的x同时带进去，这是可以同步进行的，但是后面的操作态保证了：因为只有f（x）=1的时候，它一翻转就会带来一个—1，就给你那个目标x做标记，目标态前面一个—1，而其它态没有。

你当然可以说你一下子没有找出来，因为这些态出来还是叠加的，但是你一动脑筋这个算法就出来了，比如说我有100万的数据，我在这里找，那我先用50万带进去，我发现没标记，我把这50万扔掉，这50万肯定没有的，我后带进去50万，我发现结果态变了，产生一个负号，那马上就可以取出来，再把这50万数据分成两部分，迭代下去，最后就能用少得多的步骤解出目标。

这样的话2的N次方的问题，又变成N步就能解决了，那这个搜索，他要有量子计算机的话，本来在北京3000万人里面，找出一个人来，本来计算量绝对巨大的，但是在量子算法里面，不会超过100步就能解决出来。

量子电路就是这样的[17]：

这个输入就是N个Q比特，这都是非定域的，所以它是2的N次方同时输入。下面那个输入的操作态是负责做标记Oracle的，把操作态取成（7）式那样的0-1态是很巧妙的，做了标记以后，虽然给前面的目标态x带来一个负号，但是它本身并没有变，这个操作态是可以永远保持的。

所以量子计算机最根本的指标就是你到底有多少个量子比特能够保持相干叠加，这是最难的。

我们来看一下拿量子的搜索搜索为比特币挖矿会怎么样，比特币挖矿刚才也说，那些矿工都是麦克斯韦妖，他们来干就是去竞争每10分钟的全网唯一合法记账权，谁竞争到这个，他的区块计的账只要时间戳不错，全网其它矿工核对，就变成唯一合法的这10分钟的区块账目。

这个过程经典算法是这样的：

Miner have a number: d;

1.Using a stochastic number: x（nonce）have (d + x);

2.Substituting (d + x)into hash function: h = h（ r + d）;

3.Compare: if h ＜ target, success;

4.If not, from first step continue again.

这个一般来讲，现在全网比特币算力是将近2000个P，这个难度是2的68次方上，已经是天文数字了，你要竞争到这个合法记账权很不容易，成本很高，因为这个除了暴力计算没有别的办法。

但是如果用量子搜索算法这个事怎么去干？



如果用量子搜索算法开始挖矿，我不会一个一个去试，你有这么多随机数，我取一半，如（8），操作态还是取（7）一样的，如果带入哈希函数值小于那个target值就翻转，就做了一个标记Oracle，最后测量，如果出现翻转的话这个态，那带入的随机数里有我们要找的值的，那我把它留下，我再取一半，以至最后找到那个随机数。本来2的68次方难度的问题，我们理论上最少68次就可以找到，这样量子计算如果实现（制造出量子芯片），会对整个的挖矿产业有本质上的影响。

谷歌现在宣称到2017年底，他会造出2的50次方的量子比特的计算芯片，比特币现在的挖矿的难度是2的68次方。

你哪怕就是先做出了七个量子比特的芯片，2的7次方，这样的量子矿机效率会比经典计算矿机提高上百倍。

10.1

**参考文献：**

【1】Tonomura A,Endo J,Matsuda T,Kawasaki T,Faber J Jr.Proceedings of the Conference on Neutron Scattering , New York,AIP,1982; Rev Mod Phys, 1988,60;1067.

【2】【BBC纪录片】量子力学揭秘02【生命在此】http://www.acfun.tv/v/ac1980137

【3】Berthold-Georg Englert，PHYSICAL REVIEW LETTERS 9 SEPTEMBER 1996，VOLUME77, NUMBER 11.

【4】A. Aspect, P. Grangier, G. Roger,« Experimental realization of Einstein-Podolsky-Rosen-BohmGedankenexperiment: A new violation of Bell's inequalities »,dans Physical Review Letters, Vol. 49, N. 2, {pp. 91–94 (1982)

【5】爱因斯坦1933年在牛津大学的演讲，《走近爱因斯坦》，许良英译，2005-6，辽宁教育出版社；

【6】R.P.费曼，A.R.希布斯，《量子力学与路径积分》科学出版社，1985；

【7John Preskill，《Quantum Computation》, http://www.theory.caltech.edu/\_preskill/ph229

【8】量子思维，《新发现》，2015,12；

【9】《区块链新经济蓝图及导读》 作者 Melanie Swan，龚鸣等译，韩锋主编，新星出版社 2016.1

【10】Melanie Swan,**Cognitive Applications of Blockchain Technology,** melanieswan.com

【11】A．Turing，Can a machine think? the world of mathematics. vol. 4, jr neuman,editor

【12】张礼，《量子力学的前沿问题》，清华大学出版社，2012,3

【13】Stephen Baker,<The Story ofWatson>,MARINER BOOKS, HOUGHTON MIFFLIN HARCOURT,2012;

【14】C.H.Bennett, International Journal ofTheoretical Physics, Vol. 21, No. 12, 1982l Journal of Theoretical Physics,Vol. 21, No. 12, 1982；

【15】Landauer, R. (1961)."Irreversibility and Heat Generation in the Computing Process," IBMJournal of Research and Development, 3, 183-19 I

【16】Noah Linden,1 Sandu Popescu,2, 3 AnthonyJ. Short,4 and Andreas Winter，**Quantummechanical evolution towards thermal equilibrium，http://arxiv.org/abs/0812.2385v1**

【17】Michael A.Nielsen,Isaac L.Chuang,<Quantum computation and Quantum Information>,Tsinghua Press,2015。

### 10.2从量子不可克隆原理到量子货币

**量子不可克隆定理与量子通信**

由于量子的本性的非定域不确定性，所以任意量子态的形式就应该是（以自旋1/2系统为例，a和b为任意满足归一化条件的复数），而测量受有限时空的限制，每次都只能得到定域的结果，也就是要么自旋朝上，要么自旋朝下。因此，想通过一次不破坏态的测量，而完全复制这个态，违背了量子非定域不确定的本性，这就是所谓量子不可克隆定理。

数学证明如下【36】：

假设测量的希尔伯特空间态基为， 假设测量幺正U操作在得到，测量得到，幺正操作并不会破坏量子非定域相干性，因此最后得到的态只能是：,这是一个纠缠态，完全不能达到克隆态的目的。不管最后测量结果得到的是，都不能达到克隆原态的效果。

用反证法：

如果我们的测量U操作可以克隆原态

量子不可克隆定理在量子通信中可是有极大的应用，恰恰因为一个窃听者完全无法克隆量子密钥态，所以ta不能在不破坏量子密钥态的情况下做窃听，所以，任何窃听者的行为都会导致被测量子密钥态的“塌缩”，也就是破坏了量子非定域整体性。这样，合法的接受者很容易发现，然后将“塌缩”的密钥态弃之不用。因此，量子通道传递密钥态理论上是绝对安全的，这也是墨子卫星在太空中建立量子通道的意义。

再一次强调，量子密钥态是可以通过量子纠缠瞬间传递的，但这不意味着违反相对论，因为这样的量子态隐形传输完全不能传递定域信息，真正加密了的信息还是需要通过经典信道传递的。下一节我们将介绍，Jonathan Jogenfors怎样通过量子不可克隆定理结合区块链，设计出量子货币。

来自瑞典的Linköping 大学的Jonathan Jogenfor一个基于量子不可克隆原理的区块链设计【35】，它拥有了某些量子计算的特点，大大提高了区块链的效率。

我们知道量子的非定域性和法则已经引起了计算机科学界各种有趣的应用，从Grover的非结构化数据库搜索的二次加速[1]，到Shor整数分解的多项式时间算法[2]。这些“量子”算法比它们的经典对应算法更快。

那么，能让量子力学帮助我们设计新的，改进的区块链体系吗？答案是肯定的。正如Wiesner已经证明的[6]，不可克隆定理[7]提供用于复制保护的有效基础。

Jonathan Jogenfor综合量子不可克隆原理与比特币的防二次支付的特点，设计出一种新的基于量子算法的区块链模式，给我们带来了启迪。

。

**Jonathan Jogenfors量子货币算法简介**

Jonathan Jogenfors量子货币核心思想是基于量子的不可克隆原理，即是任意未知量子态不可复制。量子的整体非定域性提供了一种优良的货币防拷贝技术系统。为了方便，我们在余下的内容中称传统的比特币协议为“比特币”。

**预备知识**

Jonathan Jogenfors的量子货币协议在分布式公证上仍然用一个传统的区块链，即是：每一个区块可以通过工作量证明链接到上一个区块，并且在链条中的区块可以被一个区块链浏览器阅读。但在其量子货币的区块链中，区块中只包括新产生的量子货币描述。交易在本地完成时都不会被记录。Jonathan Jogenfors使用了下面正规的定义：

定义1 一个传统的分布式账簿设计L包括以下几个经典算法：

* 算法取(s, Kpublic )作为输入，这里s代表经典序列数以及Kpublic代表经典公钥。如果序数s已经存在于区块账簿中算法失败，否则，将通过反复试验随机特定值开始解工作量证明试题。如果试题解开，算法将继续下去，这时账簿数值对(s, Kpublic )将被加入一个新的区块。
* 是一个多项式时长的算法，它取序列数s作为输入，如果发现公钥Kpublic已在账簿中就把它作为输出，否则算法失败。

接着，上述设计L将持续运行直到另一个矿工解开了下一个工作量证明问题，这对所有参与者都是重新开始的透明过程。

Jonathan Jogenfors的量子货币算法仍然使用传统的数值签名。就像比特币已经使用的256位比特的 ECDSA,但是Jonathan Jogenfors对量子货币执行一个特殊的算法取而代之，这是由Aaronson 和Christiano [15]首先提出的算法：

定义2 一个经典的公钥签名设计D包括三个概率的多项式时长经典算法：

1. KeyGenD是包括输入一个安全参数n和随机产生一个密钥对
2. SignD是包括输入一个私钥Kprivate和一个信息M并产生一个（尽可能随机的）签名SignD (Kprivate , M )。
3. 验证，对于输入的一个公钥 Kpublic，一个信息M，和一个确认签名ω,要么接受，要么拒绝。

这个密钥对(Kprivate , Kpublic )遵循通常的公钥密码学惯例：私钥是保密的，就像我们3.2介绍的：黑客攻击者是很难从公钥导出私钥的。对于Jonathan Jogenfors的量子货币算法，**私钥仅仅用于产生新的代币并且应该在算法完成后放弃。**

**隐形子空间迷你机制**

Jonathan Jogenfor量子货币算法使用了一个所谓迷你机制的模型，由Aaronson和Christiano【15】，Lutomisriski等【23】、Farhi等人【24】首倡。迷你机制只能产生和验证一个单独的量子货币，后面Jonathan Jogenfor用区块链将这种机制扩张到整个量子货币系统中。我们采用的迷你机制是通过Aaronson 和Christiano【15】提出的迷你机制隐形子空间系统。在这个机制里，量子货币是这样一种量子态：

 （1）

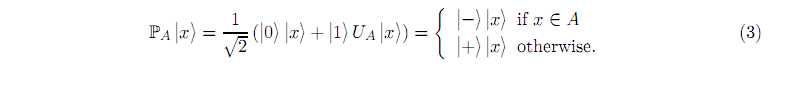
这里A是的子空间，代表一个长度为n的比特串，其子空间A是从n/2的私密生成元集合中随机产生的。同理，我们定义是A的正交补集，即是这样的y集合，如果y∈则x▪y=0,对于所有x∈。



既然我们准备确定这样的量子态代表量子货币，那么怎样识别它是要首先考虑的，因此，Jonathan Jogenfor定义刻标算符:

 （2）

这个算符用来确定对象是否属于A。接下来我们将给出这个刻标算符的操作过程。使用我们可以在A的某一组基矢上执行的投影算符，其主要作用是用作用在最后得到，即是用以下方式作用在：



其中Hadamard基：；

和是测量控制态，如果最后输出态是，我们就验证到了这个量子货币（这是不是和上节的Deustch量子算法很像？）。

可以用上面类似的方法定义和。

结合投影算符，Jonathan Jogenfor构造一个幺正算符：



这里表示空间的量子傅立叶变换。Jonathan Jogenfor用（4）定义的算符去验证量子货币态，即是则通过，则失败。

正式地，Jonathan Jogenfor定义所谓迷你机制为：

定义3 隐形迷你机制M包括两个多项式时长的算法和.

在我们详细阐述挖矿和验证算法之前，我们需要介绍一个生成和验证量子态和序列值的方法。这些算法会一般有如下结构：

定义4 一个态生成元g（r）取一个随机n比特数串r和回归,这里是一个3n比特数串和是一个对于子空间中的线性无关的生成元集合。对于子空间我们需要对于每个r都区隔开的序列数。

定义5 一个序列数验证算符H（s）取一个序列数值s并且如果对于某种正确序列值s=的时候通过，否则失败。

算法g（r）和H（s）可以用一个随机循环执行，或者就像Aaronsoon和Christiano[15,pp.32-38]介绍的那样显式的使用类似一个多重多项式机制。Jonathan Jogenfor用以下算法给出一个完整的迷你机制描述：

定义6 取一个安全参数n输入。然后它随机的生成一个能通过态生成元g（r）的n-比特私钥r。反馈值是，就是通过方程（1）产生量子比特币（s，ρ）,这里ρ=〡A〉。

定义7 验证算符取一个量子比特币C斜杠的输入，然后操作如下验证：

1. 形式验证：当且仅当C斜杠拥有形式（s，ρ）才接受，这里s是一个经典序列数并且ρ是一个量子态。
2. 序列数验证：当且仅当序列数验证算符H（s）通过时才接受；
3. 应用算符在量子态ρ上，当且仅当时才接受。

注意：如果以上任何步骤失败，验证过程将失败。

**量子货币的初级架构**

迷你机制M只能产生和验证单个量子货币，因此要建构一个可用的量子货币经济生态系统我们需要扩展这个机制来产生和验证任意数量的量子货币。为了这个目的Jonathan Jogenfor构造了一个全量子货币机制，Q，并且执行一个扩展的迷你机制M。M和Q的关系是由Aaronson和Christiano【15】，Lutomirski，Farhi【24】等人的“标准架构”来导出的。正规地，量子货币的机制定义如下：

定义8 一个公钥分布式量子货币机制Q包括以下算法：

1. KeyGenQ,一个多项式时长的算法包括一个安全参数n输入并随机产生一个密钥对（Kpublic,Kprivate）.

2.MintQ取一个安全参数n和一个私钥并且产生一个量子货币$.

3.VerifyQ是一个多项式时长的验证算法，它输入一个发布的量子比特币态C斜杠和一个对应的公钥Kpublic，要么接受，要么拒绝。

对于给定的迷你机制M=,一个数字签名机制D=和一个分布式账簿机制L=,首先可以直接架构一个版本的量子货币机制Q==。接下来，Jonathan Jogenfor将拓展这个架构以抵御重复使用攻击。

在开始架构之前，我们定义是一个简单的数字签名机制。接下来，我们定义验证已发布量子比特币C斜杠的算法：

1、检验C斜杠是具有形式（s，ρ，σ），这里s是一个经典序列数，ρ是一个量子态，σ是一个经典数字签名。

2、我们用通过序列值s检索到公钥Kpublic；

3、我们用去验证量子比特币的数字签名；

4、在迷你机制中使用。

当且仅当上述步骤都通过时，验证算法才算被通过。Jonathan Jogenfor量子货币结构设计的主要挑战在于现在矿工不需要是信任节点，而过去的量子货币系统是要假设矿工都是信任节点，比如银行。和比特币的精神一致，Jonathan Jogenfor希望通过共识算法让独立的非信任矿工组成一个可信任集团【8】。第一步，受比特币启发的挖矿算法现在设计如下：

1、用随机的产生一个密钥对（Kprivate，Kpuclic）；

2、用产生一个候选量子比特币，并反馈（s，ρ），这里s是经典序列数，ρ是量子态；

3、对序列数签名：

4、使用将序列数s和公钥Kpublic添加进账簿；

5、如果操作失败，重新从第2步开始运行；

6、如果序列数被成功添加，输入序列数，量子态和签名将一起产生量子比特币$=(s,ρ,σ).

我们可以马上确定Jonathan Jogenfor量子货币的第一个主要优点。本来比特币需要把每笔交易都记录在区块链中-一个非常费时的过程。量子货币交易马上完成。根据量子力学不可克隆原理，量子货币下的量子态不可能被复制，因此防止了被假造复制。

**防止重复使用攻击**

Jonathan Jogenfor首先尝试使用算法，但是出现了一个问题。在量子货币中，不需要信任前提，因此用户在产生量子货币的时候不再像Aaronson 和Christiano【15】当初假设的那样一定遵守规则。这会导致一个弱点，就是存在重复使用攻击问题：理想状态中，即使提供两次同样的论证，挖矿算法和态生成都是不可预测的。不幸的是，我们假设算法每一步都是确定的，只有明显除外。因此，存在邪恶矿工产生一个量子货币，并把它记账在区块链，偷偷的重复使用私钥产生任意数量的量子货币并通过验证的可能。

这是一个很严重的问题。

Jonathan Jogenfor为防止重复使用攻击采取了附加的挖矿二次算法，就是把数据也同时记入一个新的账簿L’。对于挖矿二次算法，他引入安全参数m≥1并且，具体算法如下：

1、一个矿工（这时应该被称为量子飞片矿工）仍用上面的原始挖矿机制，但是最终产生量子飞片（s，ρ，σ）；

2、量子飞片矿工把量子飞片在交易所出售；

3、另一个矿工（应被称为量子货币矿工）在交易所购买了m个量子飞片,对于所有,满足以下条件：

* 接受；
* 量子飞片在量子飞片账簿L中的时间戳T满足,这里t是当前时间；

4、量子货币矿工用随机的产生一对密钥（Kprivate，Kpublic）；

5、量子比特币矿工取m个量子飞片的序数值综合经典描述符s=并签名.

6、量子比特币矿工取m个量子飞片并结合签名，产生一个候选量子比特币;

7、量子货币矿工使用结合量子货币矿工的公钥Kpublic和经典描述符s写入账簿中。这里，如果任何m个量子飞片已经结合量子货币存在于这个账簿L’中，写入失败。

10.2

参考文献：

[1] L. K. Grover. “A Fast Quantum Mechanical Algorithm for Database Search”. In: Proceed-

ings of the Twenty-eighth Annual ACM Symposium on Theory of Computing. STOC ’96.

New York, NY, USA: ACM, 1996, pp. 212–219. isbn: 978-0-89791-785-8. doi: 10.1145/237814.237866.

[2] P. W. Shor. “Algorithms for Quantum Computation: Discrete Logarithms and Factoring”.

In: Proceedings of the 35th Annual Symposium on Foundations of Computer Science. Santa

Fe, NM: IEEE Computer Society Press, Nov. 1994, pp. 124–134.

[3] C. H. Bennett and G. Brassard. “Quantum cryptography: Public key distribution and coin

tossing”. In: Proc. of the IEEE Int. Conf. on Computers, Systems, and Signal Processing.

175textendash179. Bangalore, India: IEEE New York, 1984.

[4] A. K. Ekert. “Quantum cryptography based on Bell’s theorem”. In: Phys. Rev. Lett. 67

(1991), pp. 661–663. doi: 10.1103/PhysRevLett.67.661.

15[5] A. Broadbent and C. Schaﬀner. “Quantum cryptography beyond quantum key distri-

bution”. In: Designs, Codes and Cryptography 78.1 (Dec. 21, 2015), pp. 351–382. issn:

0925-1022, 1573-7586. doi: 10.1007/s10623-015-0157-4.

[6] S. Wiesner. “Conjugate Coding”. In: SIGACT News 15.1 (Jan. 1983), pp. 78–88. issn:

0163-5700. doi: 10.1145/1008908.1008920.

[7] W. K. Wootters and W. H. Zurek. “A single quantum cannot be cloned”. In: Nature

299.5886 (Oct. 28, 1982), pp. 802–803. doi: 10.1038/299802a0.

[8] S. Nakamoto. “Bitcoin: A peer-to-peer electronic cash system”. In: Consulted 1.2012

(2008), p. 28.

[9] K. Okupski. “Bitcoin Developer Reference”. In: (2015).

[10] A. Back. “Hashcash, a denial of service counter-measure”. In: (Aug. 1, 2002).

[11] J. R. Douceur. “The Sybil Attack”. In: Peer-to-peer Systems. Springer, 2002, pp. 251–260.

[12] G. O. Karame, E. Androulaki, and S. Capkun. “Double-spending Fast Payments in Bit-

coin”. In: Proceedings of the 2012 ACM Conference on Computer and Communications

Security. CCS ’12. New York, NY, USA: ACM, 2012, pp. 906–917. isbn: 978-1-4503-1651-4.

doi: 10.1145/2382196.2382292.

[13] K. Kaskaloglu. “Near Zero Bitcoin Transaction Fees Cannot Last Forever”. In: (2014).

[14] G. Brassard. “Brief history of quantum cryptography: A personal perspective”. In: Theory

and Practice in Information-Theoretic Security, 2005. IEEE Information Theory Work-

shop on. IEEE, 2005, pp. 19–23.

[15] S. Aaronson and P. Christiano. “Quantum Money from Hidden Subspaces”. In: (Mar. 21,

2012). arXiv:1203.4740.

[16] C. H. Bennett, G. Brassard, S. Breidbart, and S. Wiesner. “Quantum Cryptography, or

Unforgeable Subway Tokens”. In: Advances in Cryptology. Ed. by D. Chaum, R. L. Rivest,

and A. T. Sherman. Boston, MA: Springer US, 1983, pp. 267–275. isbn: 978-1-4757-0604-8

978-1-4757-0602-4. doi: 10.1007/978-1-4757-0602-4\_26.

[17] F. Pastawski, N. Y. Yao, L. Jiang, M. D. Lukin, and J. I. Cirac. “Unforgeable Noise-

Tolerant Quantum Tokens”. In: Proceedings of the National Academy of Sciences 109.40

(Oct. 2, 2012), pp. 16079–16082. issn: 0027-8424, 1091-6490. doi: 10.1073/pnas.1203552109.

arXiv:1112.5456.

[18] A. Brodutch, D. Nagaj, O. Sattath, and D. Unruh. “An adaptive attack on Wiesner’s

quantum money”. In: (Apr. 5, 2014). arXiv:1404.1507.

[19] M. Mosca and D. Stebila. “Uncloneable quantum money”. In: Canadian Quantum Infor-

mation Students’ Conference (CQISC). 2006.

[20] M. Mosca and D. Stebila. “A framework for quantum money”. In: Quantum Information

Processing (QIP). Brisbane, Australia, 2007.

[21] M. Mosca and D. Stebila. “Quantum Coins”. In: (Nov. 6, 2009). arXiv:0911.1295.

[22] S. Aaronson. “Quantum Copy-Protection and Quantum Money”. In: 24th Annual IEEE

Conference on Computational Complexity, 2009. CCC ’09. 24th Annual IEEE Conference

on Computational Complexity, 2009. CCC ’09. July 2009, pp. 229–242. doi: 10.1109/CCC.2009.42.

[23] A. Lutomirski, S. Aaronson, E. Farhi, D. Gosset, A. Hassidim, J. Kelner, and P. Shor.

“Breaking and making quantum money: toward a new quantum cryptographic protocol”.

In: (Dec. 20, 2009). arXiv:0912.3825.

[24] E. Farhi, D. Gosset, A. Hassidim, A. Lutomirski, and P. Shor. “Quantum money from

knots”. In: (Apr. 28, 2010). arXiv:1004.5127.

16[25] A. Lutomirski. “Component mixers and a hardness result for counterfeiting quantum

money”. In: (July 1, 2011). arXiv:1107.0321.

[26] J. Garzik. Making Decentralized Economic Policy. BIP 100 - Theory and Discussion, v0.8.1.

June 15, 2015.

[27] F. Reid and M. Harrigan. “An Analysis of Anonymity in the Bitcoin System”. en. In:

Security and Privacy in Social Networks. Ed. by Y. Altshuler, Y. Elovici, A. B. Cremers,

N. Aharony, and A. Pentland. New York, NY: Springer New York, 2013, pp. 197–223.

isbn: 978-1-4614-4138-0 978-1-4614-4139-7.

[28] S. Meiklejohn, M. Pomarole, G. Jordan, K. Levchenko, D. McCoy, G. M. Voelker, and S.

Savage. “A Fistful of Bitcoins: Characterizing Payments Among Men with No Names”. In:

Proceedings of the 2013 Conference on Internet Measurement Conference. IMC ’13. New

York, NY, USA: ACM, 2013, pp. 127–140. isbn: 978-1-4503-1953-9. doi: 10.1145/2504730.2504747.

[29] M. Moser, R. Bohme, and D. Breuker. “An inquiry into money laundering tools in

the Bitcoin ecosystem”. In: IEEE, Sept. 2013, pp. 1–14. isbn: 978-1-4799-1158-5. doi:

10.1109/eCRS.2013.6805780.

[30] “BitIodine: Extracting Intelligence from the Bitcoin Network”. en. PhD thesis. Aug. 2013.

[31] D. Kondor, M. Pósfai, I. Csabai, and G. Vattay. “Do the Rich Get Richer? An Empirical

Analysis of the Bitcoin Transaction Network”. en. In: PLoS ONE 9.2 (Feb. 2014). Ed. by

M. Perc, e86197. issn: 1932-6203. doi: 10.1371/journal.pone.0086197.

[32] E. Androulaki, G. O. Karame, M. Roeschlin, T. Scherer, and S. Capkun. “Evaluating

User Privacy in Bitcoin”. en. In: Financial Cryptography and Data Security. Ed. by A.-R.

Sadeghi. Lecture Notes in Computer Science 7859. Springer Berlin Heidelberg, Apr. 2013,

pp. 34–51. isbn: 978-3-642-39883-4 978-3-642-39884-1. doi: 10.1007/978-3-642-39884-1\_4.

[33] J. Rompel. “One-way Functions Are Necessary and Suﬃcient for Secure Signatures”.

In: Proceedings of the Twenty-second Annual ACM Symposium on Theory of Comput-

ing. STOC ’90. New York, NY, USA: ACM, 1990, pp. 387–394. isbn: 978-0-89791-361-4.

doi: 10.1145/100216.100269.

[34] S. Aaronson. “Limitations of Quantum Advice and One-Way Communication”. In: (Feb. 14,

2004). arXiv:quant-ph/0402095

【35】Jonathan Jogenfors，Quantum Bitcoin: An Anonymous and Distributed Currency Secured by the No-Cloning Theorem of Quantum Mechanics，http://arxiv.org/abs/1604.01383v1

【36】Michael A.Nielsen,Isaac L.Chuang,<Quantum computation and Quantum Information>,Tsinghua Press,2015

### 10.3区块链描述了量子关联的资本特性

区块链的产生，是人类计算科学和密码学发展到一定高度的结晶。

而量子计算和量子密码学的出现，必然给区块链下一步的发展带来巨大的动力和前景。

但我们在这里要总结和展望的是：量子力学带给区块链的，不仅仅是技术上的某种改良和选项，而是提供了一个升级版的财富观。

正如经济日报集团的记者黄芳芳，在听懂了我关于量子力学与区块链发展关系的讨论之后，以一种相当伟大的女性直觉总结说：“从量子力学的角度看，我们眼见的实物只是世界的一部分，背后隐藏着错综复杂又符合逻辑的纠缠关系，这其实也是资产的一部分，需要数理环境加以描述。”

其实，关系、信息、人情、声誉，这些都是经济活动中极为重要的资源，但是在传统的经济计量中，这些从来不能进入计算范畴，也从来不作为资产对待，当然更形不成相应的资本市场。

这一方面是因为人们的观念，另一个更本质的原因，正如阿里研究院专家委员会副主任周子衡分析的，传统的资本市场是以中心化的柜台账户为依托，靠财务报表来运行，这个经济计量系统，由于成本高昂，几乎只能用来处理原子资产，或者顶多加上一些数据化的权益资产（但一定有原子资产对应）。

正如周子衡所指出的【1】：网络新经济的主要特点，是把传统的柜台账户体系，变成了网络账户体系。数字信息第一次进入了人们的资产视野，就像那些大互联网公司市值那么高，绝对不是说他们有多少原子资产，是因为他们掌握了大数据关联资源。

但是大互联网公司仍然是一种中心化的数据处理方式，并不能为每个用户的数据关系进行确权。

秘鲁总统的经济顾问Hernado De Sato，在他那本著名的《资本的秘密》中【2】，科学的分析了，第三世界国家为什么穷？是因为缺乏发达国家的一整套对个人资产确权并有效保护的法律和制度体系，因此无法形成发达的资本市场。

耶鲁大学教授陈志武，反复向人们讲述的一个金融事实就是：完善的资本市场是美国人民大部分财富的来源。

作为我们中国人，最确实的体会是，三十年前我们几乎没有对房地产确权，所以没有房地产市场。但是现在哪怕只是对房地产部分的确权，形成的市场已经让我们很多人的财富状况有了天翻地覆的变化！

那么对我们每个人的数据和关系确权呢？

靠中心化的确权方式显然做不到，因为成本无法覆盖，但去中心化的区块链却开始做到了。

比特币，在人类历史上第一次做到了，对于互联网上的数字进行确权，并确保了转移的唯一合法性。比特币开启了让数字作为资产的时代。比特币也从本来就是一串哈希数字，变成了目前市值超过一百亿美元，并很可能继续快速膨胀的资本体系。

以太坊，以区块链上的智能合约做到了，为全球任何两点之间的经济关系进行确权，未来人们的朋友圈很可能成为他们资产的重要组成部分。

为什么区块链能大幅度降低金融成本？看看中国矿工的行为（区块链矿工的全网公证记账是其建立信用的基础），TA们跑到四川新疆等最偏僻慌凉的地方，建立了矿场，正为全球生产成本最低的信用资源。这和传统银行必须到北京金融街、上海陆家嘴盖高楼大厦取信于人，真是大异其趣。

所以，有了区块链，有了这样的技术，人类的资产财富观，升级到量子非定域关联的高度，有了基础。

而计算，不管是经典计算，还是量子计算，都无疑是这一历史进程的加速器。

10.3

参考文献

【1】周子衡序，韩锋、张晓枚主编，《区块链——金融史和量子计算的视角》，机械工业出版社（将出版）；

【2】Hernado De Soto,<The Mystery of Capital>,2003