

热链经济白皮书

V0.4

Prepared by	William A. H. Kuo	Date	2018-4-25
拟制		日期	
Approved by	黄发隆	Date	2018-5-1
批准人		日期	

热链团队

All rights reserved
版权所有 侵权必究

Table of Contents

1 量子时代的技术应用领域	6
前言	6
1.1 科学技术是第一生产力	6
1.2 量子计算机	6
1.2.1 摩尔定律正走向终结.....	6
1.2.2 量子计算.....	7
1.2.3 量子计算机原型.....	8
1.2.4 量子计算机应用领域.....	8
1.2.5 量子芯片研究的国际国内现状.....	9
1.3 量子通信	10
1.3.1 传统通信隐患.....	11
1.3.2 现代密码学与无条件安全.....	12
1.3.3 量子通信技术迅猛发展.....	12
1.3.4 世界各国在量子加密通信方面的战略部署.....	14
1.3.5 矛与盾：后量子密码技术 PQC.....	15
1.4 量子传感和测量	17
1.4.1 量子传感和测量.....	17
1.4.2 量子传感器的概念与现状.....	17
1.4.3 量子传感器的市场应用.....	18
1.4.4 量子传感技术商业化前瞻.....	19
1.5 量子成像和量子雷达	20
1.5.1 量子成像技术.....	20
1.5.2 重构看不到的世界.....	20
1.5.3 量子雷达技术.....	21
1.5.4 量子成像的市场空间.....	21
1.6 量子化学应用	22
1.6.1 量子化学基本原理和应用.....	22
1.6.2 光电材料的分子设计.....	23
1.6.3 碳笼化学与物理.....	24
1.6.4 含能材料在军事和航天的应用进展.....	24
1.7 量子钟	25
1.7.1 什么是原子钟?	25
1.7.2 原子钟商业应用.....	25
1.7.3 量子钟国际备战.....	26
2 什么是热链.....	27

3	热链“区块链+量子技术”生态体系发展	28
3.1	从量子技术到区块链的哲学思考	28
3.2	热链生态圈-量子技术商业化产学研联盟	31
3.3	产业化促进平台	34
3.3.1	社区基础服务平台	35
3.3.2	热链分布式应用 DApp	36
3.3.3	授权的联盟区块链网络	36
3.4	热链区块链的技术架构	37
3.4.1	协议层	37
3.4.2	主要能力框架层	37
3.4.3	接口服务层	37
3.4.4	核心应用层	39
3.4.5	热链通证的过渡方案	39
4	热链 Token 发行重要事项探讨.热链通证系统--量子信息技术资产的代币机制	39
4.1	热链通证系统--量子信息技术资产的代币机制	39
4.1.1	热点的分配与发行	39
4.2	量子商业化和收益回报体系	40
5	热链的治理机制	40
5.1	治理机制	41
5.1.1	热链社区大会	42
5.1.2	节点管理委员会	42
5.2	风险管控	42
5.3	财务管理与审计	42
6	热链团队及顾问	44
6.1	团队介绍	44
6.2	专家顾问	44
7	热链 HEATCHAIN 发展历程及项目时间规划	45
8	总结与展望	46

List of Tables

表格 1 全球主要发达国家和地区量子通信领域技术保障	14
表格 2 量子传感器的性能分析.....	18

List of Figures

图 1 量子计算机原型	8
图 2 美军海军舰艇前所未见的海底“超级特务”性能	11
图 3 BB84 协议流程说明	13
图 4 量子传感与测量的广泛应用领域.....	17
图 5 热链生态体系活力制备模型.....	31
图 6 热链生态体系规划.....	32
图 7 热链整体系统架构规划图.....	37

前言

2016 年 8 月 16 日，中国成功发射了世界上第一颗量子科学实验卫星“墨子”号。似乎也正是从这一天开始，标志着“量子”概念开始走进中国公众的视野。



图 1 墨子号量子通信卫星

那么，“量子”究竟是什么？量子就是“离散变化的最小单元”。

量子力学起源于 1900 年，当普朗克在研究“黑体辐射”问题时，发现在微观世界里，很多物理量都是离散变化的。同时发现必须把辐射携带的能量当作离散变化的，才能推出跟实验一致的公式。在此基础上，爱因斯坦、玻尔、德布罗意、海森堡、薛定谔、狄拉克等人提出了一个又一个新概念，大大扩展了量子力学的应用范围。到 20 世纪 20 年代末，量子力学的理论大厦已基本建立起来，能够对微观世界的很多现象作出定量描述了。

量子力学和相对论是 20 世纪两大科学革命，对人类的世界观产生了强烈的震撼。相对论在物体在以接近光速运动时以及强引力场条件下，有基础性的作用。可是，这样的状况在日常生活中几乎碰不到。大多数情况下，我们研究的对象还是在做物理学意义上的低速运动（远低于光速），地球的引力场也不强。所以，目前相对论的应用，局限在宇宙学、原子钟、全球定位系统等少数领域。描述微观世界则必须用量子力学。不仅研究原子、分子、激光这些微观对象时必须用量子力学，而且研究宏观物质的导电性、导热性、硬度、晶体结构、相变等性质时也必须用量子力学。

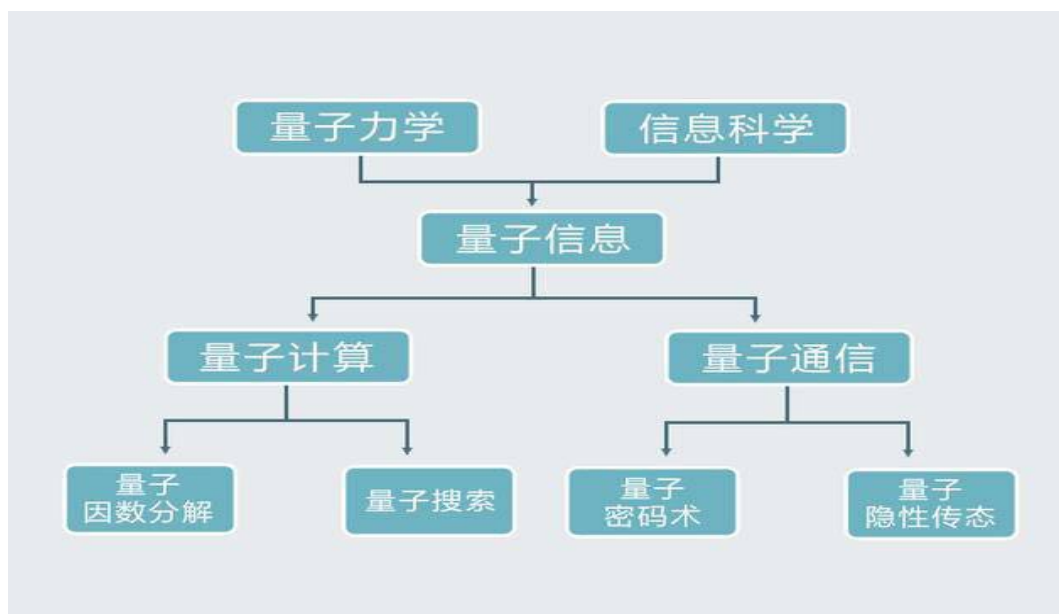


图 2 量子信息学科构成

许多最基本的问题，是量子力学出现后才能回答的。例如：

为什么原子能保持稳定，例如氢原子中的电子不落到原子核上？

为什么原子能形成分子，例如两个氢原子聚成氢气分子？

为什么原子有不同的组合方式，例如碳原子能组合成石墨、金刚石、足球烯、碳纳米管、石墨烯？为什么食盐会形成离子晶体？

为什么有些物质很稳定，而有些物质很容易发生化学反应？

为什么有些物质，如铜，能导电？有些物质，如塑料，不导电？为什么有些物质如硅，是半导体？为什么有些物质，如水银，在低温下变成超导体？

为什么会有相变，例如水在 0°C 以下结冰， $0\sim 100^{\circ}\text{C}$ 是液体， 100°C 以上气化？

为什么改变钢铁的组成，能制造出各种特种钢？

为什么激光器和发光二极管能够发光？

为什么化学家能合成比大自然原有物质种类多得多的新物质？

为什么通过观察宇宙中的光谱线能知道远处星球的元素组成？

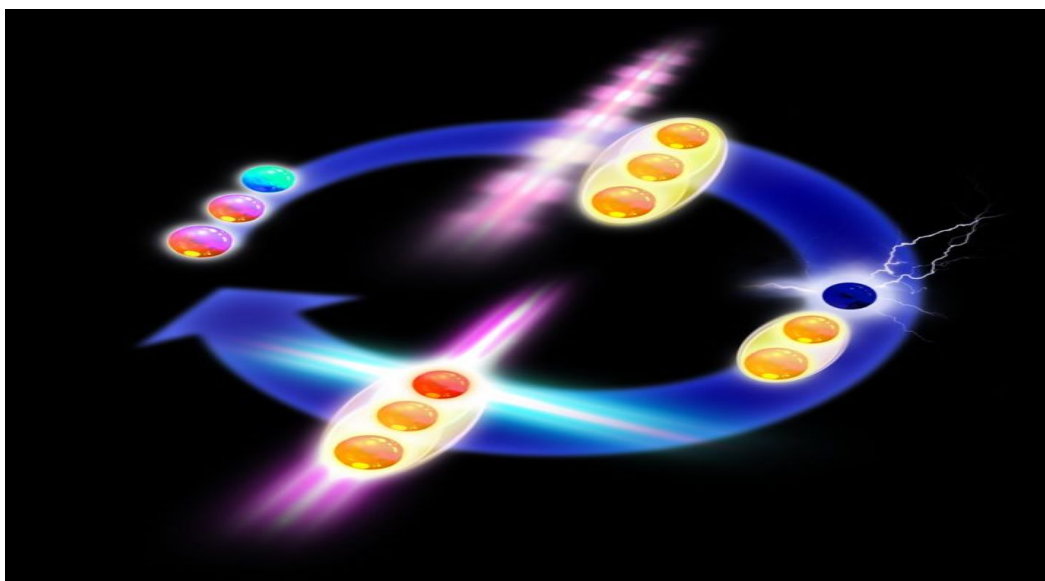


图 3 量子原理

现代社会硕果累累的技术成就，几乎全都与量子力学有关。你打开一个电器，导电性是由量子力学解释的，电源、芯片、存储器、显示器的工作原理是基于量子力学的。走进一个房间，钢铁、水泥、玻璃、塑料、纤维、橡胶的性质是由量子力学决定的。登上飞机、轮船、汽车，燃料的燃烧过程是由量子力学决定的。研制新的化学工艺、新材料、新药，都离不开量子力学。可以这么说：与其问量子力学能用来干什么，不如问它不能干什么！

1 量子时代的技术应用领域

1.1 科学技术是第一生产力

科学技术是第一生产力。尤其是前沿科技，对经济发展起首要的变革作用，向来也是各个国家关注的重点之一。现代科学技术广泛渗透到经济活动中，渗透到社会生产的各个环节，决定了它成为推动经济发展的决定性因素。层出不穷的各种新技术和应用领域，尤其是前沿科技，向来是各个国家关注的重点之一。

量子技术的时代已经到来。从量子技术在计时、传感、成像、通讯、计算和化学各领域的应用中可以看到，量子技术能够克服解决许多依靠常规技术解决不了的难题。整合国家、科研、投资和产业等各方面资源优势，在量子技术的研究和开发中发挥主导作用，确保优秀的研究成果商业化，不断挖掘新产品和新服务的潜力和价值，我们就有机会发展成世界级的工业，获得更多跨学科、懂需求、技术精湛的量子技术科技大军的鼎力支持，从而形成能够中国领先并可持续增强优势的一系列应用领域。相比传统计算机，量子计算机是一种原理上的颠覆式超越。理论上讲，量子计算机可以将传统计算机数万年才能处理的复杂问题，几秒钟就解决。在量子理论诞生 118 年之后，谁先夺取“量子霸权”，谁就掌握了技术制高点、标准制定权和舆论主导权，在产业竞争中占据有利地位。

据英国政府的统计报告显示，中国量子科研论文发表量排名全球第一、专利应用排名第二。凭借着潘建伟、郭光灿等领军科学家及团队的一系列重大突破，如今的中国已站在世界量子信息科研的舞台中央。近两年来，中国发射了世界首颗量子通信科学实验卫星，首次实现千公里量子纠缠，成功研发全球首台超越早期经典计算机的光量子计算机。

1.2 量子计算机

1.2.1 摩尔定律正走向终结

“摩尔定律”归纳了信息技术进步的速度，是由英特尔（Intel）创始人之一戈登·摩尔（Gordon Moore）提出来的。其内容为：当价格不变时，集成电路上可容纳的元器件的数目，约每隔 18-24 个月便会增加一倍，性能也将提升一倍。在摩尔定律应用的 40 多年里，电子计算机从神秘不可近的庞然大物变成多数人都不可或缺的工具，信息技术由实验室进入无数个普通家庭，因特网将全世界联系起来，多媒体视听设备丰富着每个人的生活。

摩尔定律很贴切地反映了信息技术行业发展。但“杞人忧天”的物理学家们，却提出了一个“大煞风景”的问题：

一是巨大的能耗，芯片有被烧坏的危险。芯片发热主要是因为计算机门操作时，其中不可逆门操作会丢失比特。物理学家计算出每丢失一个比特所产生的热量，操作速度越快，单位时间内产生的热量就越多，计算机温度必然迅速上升，必须消耗大量能量来散热，否则芯片将被烧坏。

二是为了提高集成度，晶体管越做越小，当小到只有一个电子时，量子效应就会出现。电子将不再受欧姆定律管辖，由于它有隧道效应¹，本来无法穿过的壁垒也穿过去了，所以量子效应会阻碍信息技术继续按照摩尔定律发展。

这两个限制就是物理学家们预言摩尔定律会终结的理由所在。

1.2.2 量子计算

工程专家一直尝试用不同的方法保持计算机处理性能快速增长，其中量子计算就是提高计算机处理性能最好的办法之一。量子计算理论如今已经在实验室被证实，其性能超越目前所有的超级计算机，然而真正的进入产业化阶段还需要一定的时间进行发展。

量子计算的概念最早是 1982 年由美国物理学家费曼提出的。1985 年，英国物理学家又提出了“量子图灵机”的概念，之后许多物理学家将“量子图灵机”等效为量子的电子线路模型，并开始付诸实践。真正使世人正身注意量子计算机的是彼得·秀尔（Peter Shor）在 1994 年发表的一篇论文，他当时在贝尔实验室工作。秀尔博士证明了量子计算机可以被用来进行一个很大的数字的质因数分解。

量子计算机和电子计算机一样，其功用在于计算具体数学问题。所不同的是：

✧ 经典比特(bit)

电子计算机所用的电子存储器是经典比特，每个比特取值只能为 0 或者为 1。

✧ 量子比特(qubit)

¹隧道效应：由微观粒子波动性所确定的量子效应，又称势垒贯穿。本质上是量子跃迁，粒子迅速穿越势垒。在势垒一边平动的粒子，当动能小于势垒高度时，按照经典力学，粒子是不可能越过势垒的；而对于微观粒子，量子力学却证明它仍有一定的概率贯穿势垒，实际也正是如此，这种现象称为隧道效应。

量子计算机使用量子比特，基于量子性质，每个量子比特取值可以为 0，或者为 1，或者 0 和 1 的叠加。

所以电子计算在某个时间只能存一个数据，它是确定的，操作一次就把一个比特（bit，存储器最小单元）变成另一个比特，实行串行运算模式，N 个经典比特在同一时间只能代表一个数据；而量子计算机中一个量子比特可以同时存储两个数值，N 个量子比特可以同时存储 2 的 N 次方数据，操作一次会将这个 2 的 N 次方数据变成另外一个 2 的 N 次方数据，以此类推，运行模式为一个 CPU 的并行运算模式，运行操作能力指数上升，这是量子计算机来自量子性的优点。

1.2.3 量子计算机原型

量子计算本来就是并行运算，所以说量子计算机天然就是“超级计算机”。要想研制量子计算机，除了要研制芯片、控制系统、测量装置等硬件外，还需要研制与之相关的软件，包括编程、算法、量子计算机的体系结构等。

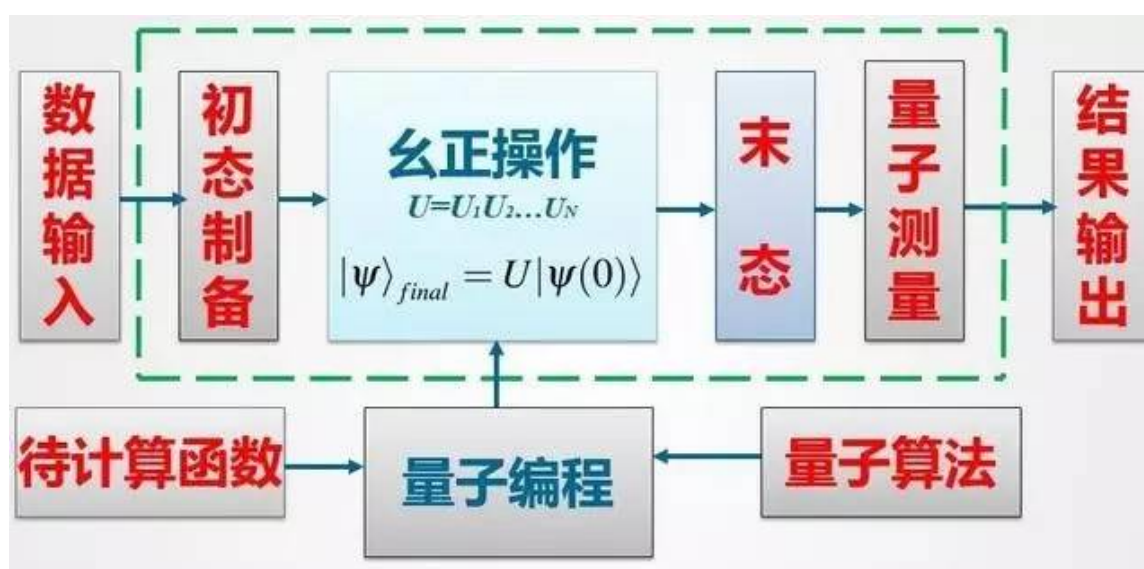


图 1 量子计算机原型

一台量子计算机运行时，数据输入后，被编制成量子体系的初始状态，按照量子计算机欲计算的函数，运用相应的量子算法和编程，编制成用于操作量子芯片中量子比特幺正操作变换，将量子计算机的初态变成末态，最后对末态实施量子测量，读出运算的结果。

这种基于“量子图灵机”的标准量子计算是量子计算机研制的主流。除此以外，还有其他量子计算模型，如：单向量子计算，分布式量子计算，但其研制的困难并没有减少。另外，还有拓扑量子计算，绝热量子计算等。

由于对硬件和软件的全新要求，量子计算机的所有方面都需要重新进行研究，这就意味着量子计算是非常重要的交叉学科，是需要不同领域的人共同来做才能做成的复杂工程。

1.2.4 量子计算机应用领域

投资者现在不仅仅是想要加入计算机行业，他们也正争相进入量子计算的生态系统。银行、航空航天公司和网络安全公司都在利用计算机革命的优势。量子计算已经对上述领域产生了影响，与所有新技术一样，随着硬件不断发展，新机会的不断出现，现在看来难以想象的应用很可能在未来成为可能。

量子计算能力十分惊人，但是这并不是仅仅说现在的软件会以十亿倍的速度运行这么简单。更确切地说，量子计算机有自己擅长的特定领域，某些类型的问题是它们擅长解决的，而有些问题则不。以下是下一代计算机普及过程中我们可以看到的一些主要应用：

✧ 人工智能

量子计算机的一个主要应用是人工智能(AI)。人工智能是基于从经验中学习的原则，根据不断给出的反馈，机器的反应会越来越准确，直到计算机程序可以算得上“智能”。人工智能会颠覆所有从汽车到医学等各个行业领域，据说 21 世纪人工智能的发展就和 20 世纪电的发明一样重要。

✧ 分子模型

另一个量子计算机能涉及的领域是在分子模型，在找到化学反应的最佳配置后对分子的相互作用进行精确建模。这种“量子化学”非常复杂，以至于只有其中最简单的分子才能被现在的数字计算机分析。化学反应是自然界的量子变化，它们构成了高度纠缠的量子叠加态。但是如果把这件事情交给高度发达的量子计算机来做，在评估哪怕是最复杂的过程时也不会有任何困难。

✧ 密码演算学

现在大部分的网络安全都是依靠将大量数据分解为素数解决问题。虽然现在可以通过使用数字计算机来搜索每一个可能的答案，但这个方法非常费时，使得“破解密码”变得昂贵而不实用。量子计算机可以比数字计算机更高效地执行这些计算，这就意味着如此保证安全的方法很快就会过时。

✧ 金融模型

金融市场是现存最复杂的系统。虽然我们已经开发出越来越多的科学和数学工具来解决这一问题，但它仍然面临着与其他科学领域都不同的一个问题：没有一个可以进行实验的受控设置。利用量子计算来解决问题的一个最直接的优势是：量子计算机固有的随机性与金融市场的随机特性是一致的。投资者希望在随机产生的大量情景下评估结果的分布情况。另一个优势是，像套利这样的金融操作可能需要很多有路径依赖的步骤，而这样做的结果是数量会很快超过数字计算机的能力。

✧ 天气预报

天气预报称，美国国家石油公司的首席经济学家罗德尼·F·威瑟认为美国近 30% 的 GDP(6 万亿美元)直接或间接接受天气影响，天气影响了食品生产、运输和零售贸易等。更加准确地预测天气对很多领域都有十分重要，比如说从灾难中为人类争取更多的时间。量子计算机可以帮助人类建立更好的气候模型，从而让人类更深入地了解人类是如何影响环境的。

✧ 粒子物理学

粒子物理学的模型通常非常复杂，需要大量的计算时间来进行数值模拟。这使得量子计算成为他们的理想之选，目前研究人员已经在利用这一点进行了研究了。因斯布鲁克大学(Innsbruck)和量子光学与量子信息研究所(IQOQI)最近使用了一个可编程的量子系统来进行这样的模拟实验。

1.2.5 量子芯片研究的国际国内现状

2004 以来，世界上许多著名的研究机构，如美国哈佛大学，麻省理工学院，普林斯顿大学，日本东京大学，荷兰 Delft 大学等都投入了很大的力量，在半导体量子点作为未来量子芯片的研究方面取得一系列重大进展。

2017 年 7 月份，美国白宫发布了《推进量子信息科学：国家的挑战与机遇》。报告中，美国国家科学技术委员会认为量子计算能有效推动化学、材料科学和粒子物理发展，未来可能最终会颠覆众多科学领域，人工智能也当属其中之一。美国联邦机构在过去的 20 年中，每年资助量子信息科学领域 2 亿美元。这些支持起到了显著的作用，让美国的科学家在该领域里处在领先地位。

英国政府科学办公室近期还发布了一份量子技术报告《量子时代：技术机会》在这份报告中，英国政府科学办公室阐述了英国如何能从量子技术中获益，并指出了“中国、美国、欧盟已经在量子科学和技术应用拥有许多的研究机构及发布了量子计划，意识到这些竞争，我们必须开放国家项目，促进英国的量子技术发展，并鼓励投资。”

基于英国国家量子技术项目取得的进展，英国政府部门强调，英国还会建立创新中心，联合学术界和工业界，未来会与国内和国际私营部门加强协调，在量子计时、成像、传感、通信和计算等领域，具备产生新产品和服务的潜力和价值。确保继续将优秀的研究成果商业化。

美国从 90 年代到现在，在基础研究阶段超导领域的突破，已经引起了企业的重视。美国所有重大的科技公司，包括微软、苹果、谷歌都在量子计算机研制领域投入了巨大的力量，以期全力争夺量子计算机这块“巨大的蛋糕”！美国的量子计算机研制之路分 3 个阶段：第一阶段政府主导，主要做基础研究；第二阶段，企业开始投入；第三阶段，加快产出速度。

其中，最典型的的就是谷歌在量子计算机领域的布局。它从加州大学圣芭芭拉分校高薪引进国际上超导芯片做得最好的 J. Martinis 团队（23 人），从事量子人工智能方面的研究。微软的量子开发工具套件 Windows 版已于 2017 年 12 月份推出，在 2018 年 2 月份，微软又针对 Mac 和 Linux 平台上的开发者推出该套件。此外，微软还开放了量子开发库和样本，并大大提高了模拟器的性能。

反观中国的量子计算机发展，仅能在国际学术界牢牢占据一席之地，产业化进程明显落后。根据郭光灿院士的报告表明，软件、材料几乎没有人做，软硬件是相辅相成的，材料研究也需提早做准备。量子计算机应当“三驾马车”一起发展，硬件、软件、材料三个都要布局。

这三驾马车，中国在集成电路、基础软件和半导体材料方面落后已久，量子计算机和量子通信将是中国奋起直追、甚至弯道超车的巨大战略窗口。

1.3 量子通信

量子通讯是近二十年发展起来的新型交叉学科，是量子论和信息论相结合的新的研究领域。量子通信主要涉及：量子密码通信、量子远程传态和量子密集编码等，近来这门学科已逐步从理论走向实验，并向实用化发展。高效安全的信息传输日益受到人们的关注。基于量子力学的基本原理，并因此成为国际上量子物理和信息科学的研究热点。

在中国，2016 年 8 月 16 日，世界首颗量子科学实验卫星“墨子号”发射成功，

2017 年 9 月 29 日，在中国科学院举行新闻发布会上，中国科学院院长白春礼就通过墨子号与奥地利地面站的卫星量子通信，与奥地利科学院院长安东·塞林格（Anton Zeilinger）进行了世界首次洲际量子保密通

信视频通话。同时宣布世界首条量子保密通信干线——

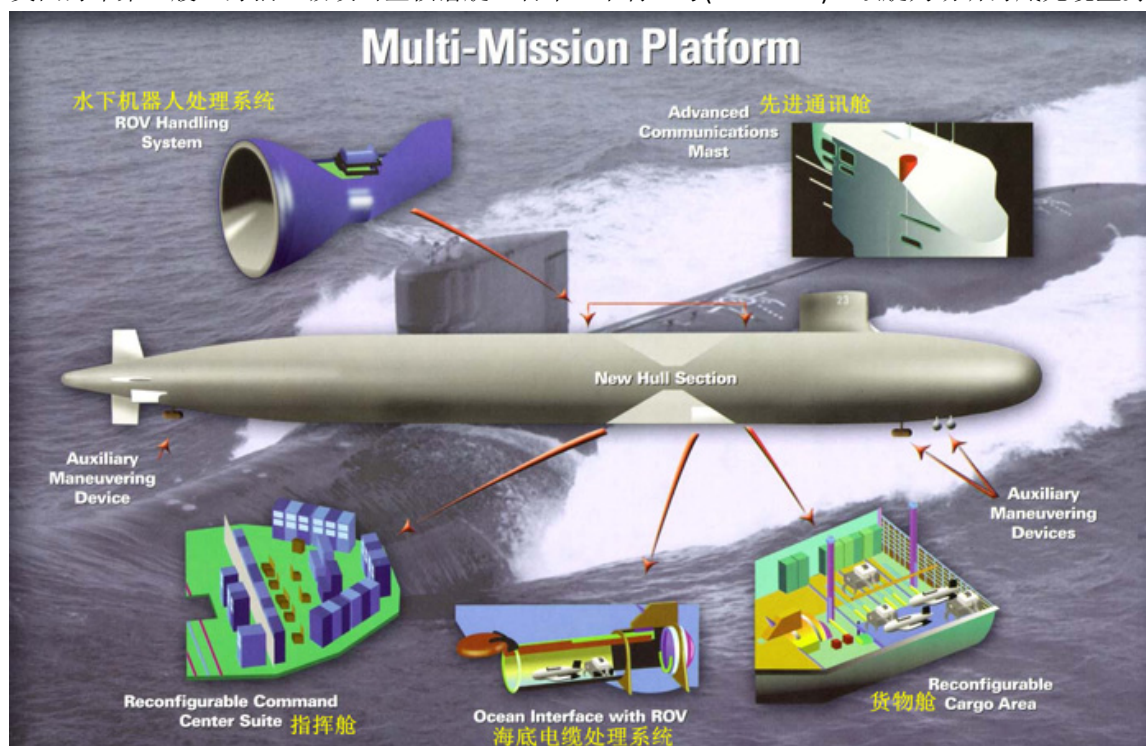
“京沪干线”正式开通。将来的目标是发射一个由 20 颗卫星组成的星座，那时就可以实现全球量子保密通信。

1.3.1 传统通信隐患

当代有线通信主要有两类介质：电缆和光纤。在电缆通信中，窃听者只需要把类似万用表或者示波器一样的东西，连接到通信电缆上，便能轻松窃听到所有信息，窃听行为不会改变和影响信息的信号，包括波形和强度等，使得窃听行为根本无法发现。虽然铜退光进，但是对于目前主流的光纤通信，也存在类似的问题。例如光纤弯曲窃听法的原理是通过将光纤弯曲，使得部分光信号外泄并被相应的探测器探测到。由于光纤损耗本来就是飘忽不定的，窃听所导致的损耗会被淹没在环境变化里，而无法被接收端察觉。

图 2 美军海军舰艇前所未见的海底“超级特务”性能

美国海军第 3 艘“海狼”级攻击型核潜艇“吉米·卡特”号(SSN-23)。该艇为窃听海底光缆量身定做



了多任务平台，搭载有最先进的电子侦察设备，可在水下搜集情报，包括对重要目标进行侦察监视和窃听海底光缆通信，因此成为美国国家安全局最理想的“水下间谍”。

自从 9.11 事件以后，美国启动了臭名昭著的棱镜计划（PRISM），它一项由美国国家安全局自 2007 年起开始实施的绝密电子监听计划。该计划的正式名号为“US-984XN”。

根据斯诺登泄露的文件，描述了 PRISM 计划能够对即时通信和既存资料进行深度的监听。许可的监听对象包括任何在美国以外地区使用参与计划公司服务的客户，或是任何与国外人士通信的美国公民。国家安全局在 PRISM 计划中可以获得的数据电子邮件、视频和语音交谈、影片、照片、VoIP 交谈内容、档案传输、登入通知，以及社交网络细节。综合情报文件“总统每日简报”中在 2012 年内在 1477 个计划使用了来自 PRISM 计划的资料。美国政府证实，它确实要求美国公司威瑞森（Verizon）提供数百万私人电话记录，其中包括个人电话的时长、通话地点、通话双方的电话号码。

信息安全问题已经受到了高度关注，动用海量软件、硬件计算资源，甚至国家力量破解现有加密系统；网络武器、网络恐怖主义和网络战争都已经迫在眉睫，因此信息保护升级刻不容缓。

1.3.2 现代密码学与无条件安全

而目前,唯一能防止传输的信息被窃听的主动手段,是对传输的信息进行加密。比如经典 **RSA** 公钥加密算法,该算法基于一个十分简单的数论事实:将两个大质数相乘十分容易,但是想要对其乘积做因式分解却极为困难,因此可以将乘积公开作为加密密钥。其破解难度很高,甚至于最快的超级计算机也无法快速破解。

信息论创始人克劳德·香农,在上世纪 50 年代对无条件安全做出过开创性的研究。他总结出了“一次一密”的无条件安全的条件,顾名思义即:

- 密钥真随机且“只使用一次”
- 与明文等长且按位进行二进制异或操作

该方法的优点是理论上不可破译,且香农进行了严格的理论证明。但其缺点是需要大量密钥,而密钥的更新和分配存在漏洞!即存在被窃听的可能性!所以不解决密钥分发的问题,就不可能实现无条件安全。这也导致了在香农发布了这一成果之后,根本没有人商业使用这种方式,据说只有莫斯科和华盛顿之间的通信,曾经使用过这种方法。

今天,科学家们可以通过量子力学原理,解决一次一密中的密钥分发问题。

1.3.3 量子通信技术迅猛发展

1984 年,IBM 公司的 Bennett 与加拿大的 Brassard 提出了量子密钥分配(Quantum Key Distribution, QKD)的新概念,以及一个量子密码分配协议-BB84 协议,标志着量子密码技术的开端。量子密码学体系包含了量子保密、量子认证、量子安全协议、量子密码分析等研究方向。主要使用的量子力学原理包括如下:

✧ 测量塌缩理论

除非该量子态本身即为测量算符的本征态,否则对量子态进行测量会导致“波包塌缩”,即测量将会改变最初的量子态。

✧ 不确定性原理

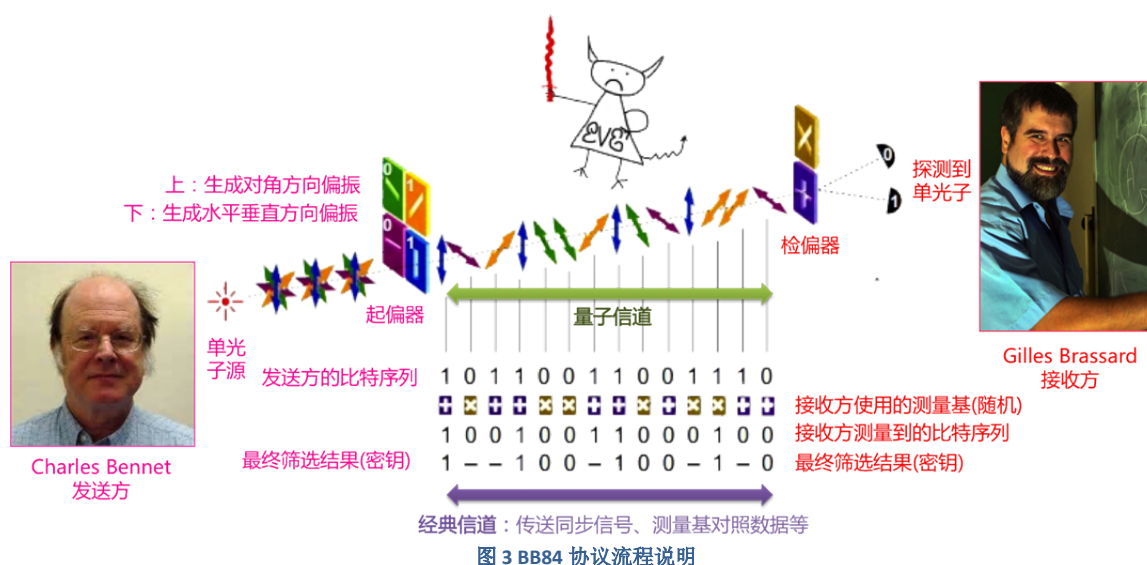
又称“海森堡不确定性原理”,即不能同时精确测量两个非对易物理量(旧称“测不准原理”)。

✧ 量子不可克隆原理

无法对一个未知的量子态进行精确的复制。

✧ 单个光子不可分

不存在半个光子。



在 2001 年，科学家从理论上证明完美的 BB84 协议，具有无条件的安全性。BB84 协议流程如下：

- 1) 发送端 Alice 随机生成上述四种密钥（垂直，水平，斜上，斜下），生成后密钥的状态即确定。
- 2) 接收端 Bob 随机使用两种测量基，对 Alice 发送的密钥进行解调。因为 Bob 随机选用测量基，所以会有一半几率选用不正确的测量基。可以看到必然会存在测量错误，那么可以计算出误码率为： $50\% \text{（选错测量基）} \times 50\% \text{（因为结果非 0 即 1，所以错误测量基有一半概率蒙对）} = 25\%$
- 3) 接收端 Bob 通过公开信道（可以被 Eve 窃听），告知 Alice 其每个码元分别对应的解调的测量基类别。然后 Alice 根据这一信息，对比自己的编码方式，就能知道自己哪些测量基选对了，哪些选错了。
- 4) 再然后，Alice 通过公开信道（可以被 Eve 窃听）告诉 Bob 需要扔掉哪些错误测量基的结果，留下的即为最终筛选结果，该结果在 Alice 端和 Bob 端相同。这两个 01 序列完全相同，即为量子密钥。

即使中间人 Eve 窃听到了公开信道上的全部信息，那么 Eve 还需窃听量子信道（先截取再重发），才能还原出最终的密钥，但这么做会造成误码率的上升，从而侦察到窃听行为的存在。

量子隐形传态（Quantum teleportation），又称量子遥传、量子隐形传输、量子隐形传送、量子远距传输或量子远传，是一种利用分散量子缠结与一些物理讯息（physical information）的转换来传送量子态至任意距离的位置的技术。是一种全新的通信方式。它传输的不再是经典信息而是量子态携带的量子信息，在量子纠缠的帮助下，待传输的量子态如同经历了科幻小说中描写的“超时空传输”，在一个地方神秘地消失，不需要任何载体的携带，又在另一个地方神秘地出现。

量子隐形传态是可扩展量子网络和分布式量子计算的基础。要实现量子隐形传态，首先要求接收方和发送方拥有一对共享的 EPR 对（即 BELL 态（贝尔态）），发送方对他所拥有的一半 EPR 对和所要发送的信息所在的粒子进行联合测量，这样接收方所有的另一半 EPR 对将在瞬间坍缩为另一状态（具体坍缩为哪一状态取决于发送方的不同测量结果）。发送方将测量结果通过经典信道传送给接收方，接收方根据这条信息对自己所拥有的另一半 EPR 对做相应么正变换即可恢复原本信息。到乙地,根据这些信息,在乙地构造出原量子态的全貌。

与广为传言的说法不同,量子隐形传态需要借助经典信道才能实现,因此并不能实现超光速通信。在这个过程中,原物始终留在发送者处,被传送的仅仅是原物的量子态,而且发送者对这个量子态始终一无所知;接受者是将别的物质单元(如粒子)制备成为与原物完全相同的量子态,他对这个量子态也始终一无所知;原物的量子态在测量时已被破坏掉—不违背“量子不可克隆定理”;未知量子态(量子比特)的这种传送,需要经典信道传送经典信息(即发送者的测量结果),传送速度不可能超过光速—不违背相对论的原理。

1.3.4 世界各国在量子加密通信方面的战略部署

作为一种抗干扰能力强、保密性好、传输速度快、信道容量大等多种优点集一身的新型通信技术,量子通信已成为国际上量子物理和信息科学与技术的研究热点,各国尤其是发达地区政府、企业和研究人员均积极地展开投入和研发。正逐渐由实验室走向市场,目前在城域及城际量子通信网络、卫星量子通信网络等领域研究应用已初见成效。

由于量子通信无条件安全性的特点,在国防、通信安全方面具有重要的作用,国外发达国家和地区争相将量子通信置于国家战略高度。

表格 1 全球主要发达国家和地区量子通信领域技术保障

国家和地区	战略政策
美国	量子通信计划 保持国家竞争力计划 信息科学白皮书 量子信息科学跨学科教师计划
欧盟	《研究与技术开发框架》,量子技术和量子通信持续作为重点研究领域 《欧洲量子科学技术》计划 《欧洲量子信息处理与通信》计划 《量子信息处理与通信战略报告(1.5 版)》,启动量子通信标准化研究
英国	国家量子技术研究项目 量子技术中心网络的投资与建设
德国	《德国 2020 高科技战略》

日本	国家级开发项目 长期研究战略,建成绝对安全保密的高速量子信息通信网
加拿大	安大略西南发展基金
马来西亚	通讯卫星 MEASAT I 和 II

美国是世界最先将量子通信试验研究和应用列入国家战略、国防和安全研发计划的国家。2003 年美国国防部高级研究计划局(DARPA)组织具有很强军方特色的美国 BBN 公司、波士顿大学、哈佛大学着手建立世界上第一个城域量子通信网络即量子保密通信与互联网结合的五年试验计划。2012 年投入 400 万美元用于设立“量子信息科学跨学科教师计划”，对有关量子信息方面的交叉学科进行研究，并开始培训储备量子通信领域跨学科人才，为接下来的发展做好人才战略储备。

1998 年欧盟在第五个《研究与技术开发框架》(1998-2002 年)中明确提出将量子技术作为发展信息社会的重点通用技术和基础研究领域。2016 年,据英国《自然》杂志网站报道,欧盟计划于 2018 年启动总额 10 亿欧元的量子技术项目,希望借此促进包括安全的通讯网络和通用量子计算机等在内的多项量子技术的发展。

2003 年日本总务省提出了以新一代量子信息通信技术为对象的长期研究战略，计划在 2020 年至 2030 年间，建成绝对安全保密的高速量子信息通信网，使保密通信网络和量子通信网络技术达到实用化水平。为推动量子通信研究，采取“产官学”联合攻关的方式，由政府引导、企业主导，高校和科研机构提供智力支持，形成上下游全面联动的研发态势，有利地助推了量子通信的开发研究。

据中国科学院院士潘建伟介绍，近年来，在国家的高度重视和大力支持之下，中国作出了一些非常有特色的工作。在量子保密通信方面，**我国已经处于全面领先的地位**，例如 2017 年 9 月 29 日，世界首条量子保密通信干线——“京沪干线”正式开通；结合“京沪干线”与量子科学实验卫星“墨子号”的天地链路，我国科学家成功实现了洲际量子保密通信。中国科学院和奥地利科学院之间举行了洲际视频会议。采用先进的加密标准，每秒刷新种子密钥。奥中视频会议历时 75 分钟，总数据传输 2GB。这标志着我国已构建出天地一体化广域量子通信网络雏形，为未来实现覆盖全球的量子保密通信网络迈出了坚实的一步。将来的目标是发射一个由 20 颗卫星组成的星座，那时就可以实现全球量子保密通信。

1.3.5 矛与盾：后量子密码技术 PQC

如果大规模量子计算机建成，可以用于破解许多目前正在使用的公钥密码系统，这将严重危及互联网等场合中数字通信的机密性和完整性。比如，300 位 10 进制那么长数，用我们目前万亿次的传统电子计算机拿来算的话，大概需要算 15 万年。但如果能够造出一台量子计算机，它计算的频率也是万亿次的话，只需要 1 秒钟就可以算完。

作为量子信息学家们的“左右手互博”绝技，后量子密码，或称抗量子密码(Post-quantum Cryptography, PQC)技术的研究目标，是发展对量子或者经典电子计算机都安全的密码系统，并且能够和已有的通信协议和网络进行互操作。

这是一个活跃的研究领域，拥有自己的系列会议，即 2006 年开始的 PQCrypto 会议。各国资助机构对后量子密码投入了大量的支持，特别是在欧洲和日本，分别有欧盟项目 PQCrypto 和 SafeCrypto，日本有 CREST 密码数学项目。

这些努力在基础研究方面取得了进展，为在现实世界中后量子密码的部署做好铺垫。在过去的几年中，行业标准组织已经开始了自己在这领域的活动：自 2013 年以来，欧洲电信标准协会(ETSI)组织了三个“量子安全密码”研讨会；在 2015 年，NIST(National Institute of Standard Technology)举行题为“后量子世界的网络安全”研讨会，有来自政府、行业和学术界的超过 140 人参加。

当前公钥密码最重要的用途是数字签名和密钥建立，建立一个大型的量子计算机将使许多公钥密码体制变得不安全，尤其包括 RSA 算法以及基于离散对数问题的密码系统。相比之下，对称密钥系统受到的影响显得不激烈，不论 Grover 算法是否有实际意义，将密钥规模增大一倍也可保证安全，此外，指数级提速的搜索算法已经被证明不可能存在，所以在量子计算时代，对称密码算法和散列函数仍然是可用的。

因此，研究能够同时抵抗传统计算机和量子计算机攻击的算法集中在公钥密码体系上。后量子密码的研究目标形成了一些主要分类，主要包括了那些基于格、代码和多变量多项式，以及少量其他的。

✧ 基于格的密码

一些振奋人心的新应用（如全同态加密、代码混淆、和基于属性的加密）已经通过基于格的密码学得到实现。大多数基于格的密钥生成算法相对简单、高效且高度可并行，同时，一些基于格的系统的安全在最坏情况的困难假设下是可证明安全的，而不是在平均情况下。另一方面，对格方案的安全进行精确估计已经被证明是困难的，即便使用已知的密码分析技术。

✧ 基于编码的密码

McEliece 密码系统自 1978 年提出后一直未被破解。自那时起，基于纠错码的其他系统陆续被提出了，但大多数基于代码的模块具有密钥规模太大的缺点，更新的改进方案尝试引入更多的结构到代码中以减少密钥规模。

✧ 多变量多项式的密码

这些方案是基于有限域上的多变量多项式系统的求解的困难性，但一些多变量密码系统已被破解，多变量多项式密码学在签名方面的应用更成功。

✧ 基于散列的签名

基于散列的签名是使用散列函数构造的数字签名方案。

✧ 其他

除上述类别，其他各类系统被相继提出。其中一个方案是基于评估超奇异椭圆曲线同源的，在椭圆曲线上的离散对数问题可以在量子计算机上用 Shor 算法有效地计算，奇异曲线同源问题不存在相似的量子攻击。

进入 2016 年，美国两家主要信息技术公司在后量子密码应用领域的活动引起了外界关注。微软公司于 4 月发布了基于格密码库（LatticeCrypto），这种可移植软件的底层机制是基于环上带误差学习问题（Ring Learning With Errors）。无论对于使用经典计算机或者量子计算机的攻击者，该软件库至少能够实现 128 位安全性能。谷歌公司也于 2016 年 7 月在官方安全博客上宣布其将开始进行后量子密码技术的测试活

动。【在对当前量子密码技术发展进行调查后，谷歌决定应用这种被称为“新希望”的基于环上带误差学习问题密钥交换协议。

密码系统的标准化工作是其大规模应用的前提。当前，多种后量子加密算法都已经在技术上具备了进行标准化的基本条件，并且包括美国国家标准与技术局在内的标准机构也开始发布后量子密码发展和迁移指导和实施计划。尽管密码标准体系的建立需要国际社会通过交流合作活动达成共识，但在密码研究领域取得领先的国家无疑将在标准制定过程中占据更多的主动权。

1.4 量子传感和测量

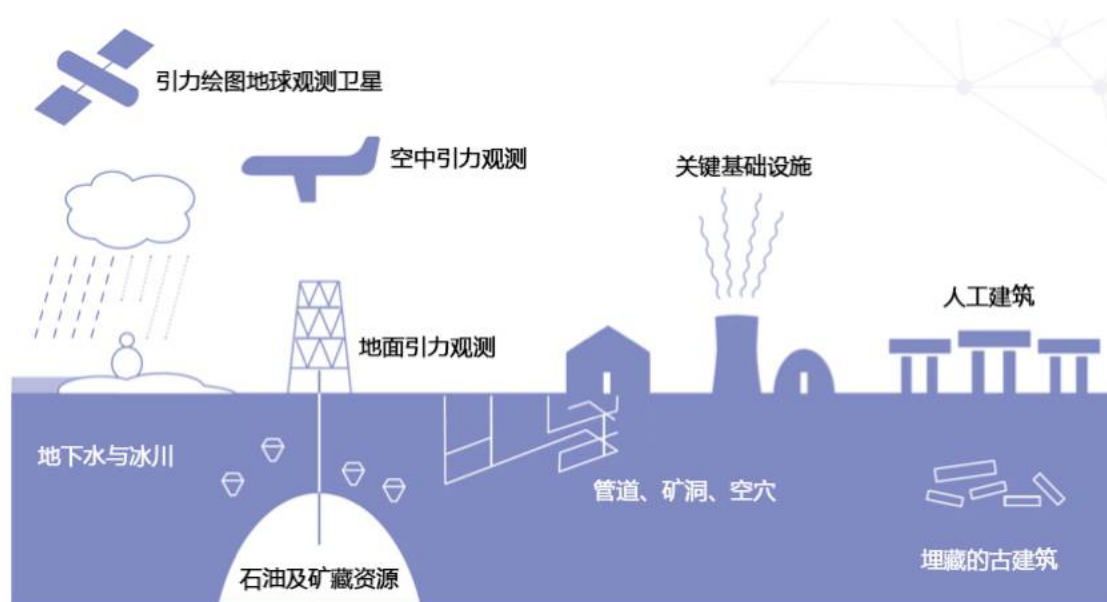
近年来量子信息学的发展，使得对微观对象量子态的操纵和控制变得越来越重要。用量子控制的理论和方法来解决量子态的控制问题从而产生了量子控制论。量子控制论是以研究微观世界系统量子态的控制问题的学科，量子传感器即可用于解决量子控制中的检测问题。

1.4.1 量子传感和测量

传感器在日常科技产品中的应用已经变得越来越广泛了，诸如在动作、声音和光线的监测领域，从数十亿枚内置于手机中的低成本运动传感器到应用于医疗保健和地球卫星系统的高端产品，传感器的身影随处可见。

而量子传感器相比于传统产品则实现性能上的“大跃进”：在灵敏度、准确率和稳定性上都有了不止一个量级的提高。也正因此，它的应用场景也变得更加多样，例如在航空航天、气候监测、建筑、国防、能源、生物医药、安保、交通运输和水资源利用等尖端领域都实现了量子传感器的商业化应用。

图4 量子传感与测量的广泛应用领域



而量子传感器的发展并非是一项技术上的单点突破，它带动的是整个生态系统的建立和完善，从工程测量到数据可视化解析，各领域即将涌现的大量工作机会都表明这一趋势已经越来越清晰。

1.4.2 量子传感器的概念与现状

与经典控制中一样，量子控制中测量的关键也是被测量和标准量的比较。而量子控制中的可观测量与量子力学中的相应自共轭算符对应，量子系统状态的直接测量一般不易实现，需要把被测量按一定的规律转变为便于测量的物理量，进而实现量子态的间接测量。这一过程可以通过量子传感器完成。

所谓量子传感器，可以从两方面加以定义：

- ✧ 利用量子效应、根据相应量子算法设计的、用于执行变换功能的物理装置；
- ✧ 为了满足对被测量进行变换，某些部分细微到必须考虑其量子效应的变换元件。

随着量子控制研究的深入，对敏感元件的要求将越来越高，传感器自身的发展也有向微型化、量子型发展的趋势，量子效应将不可避免的在传感器中扮演重要角色，各种量子传感器将在量子控制、状态检测等方面得到广泛应用。

表格 2 量子传感器的性能分析

评估体系	说明
非破坏性	因为量子控制中的状态检测与经典控制中的状态检测存在本质上的不同，测量可能引起的状态波函数约化过程暗示了对状态的测量已经破坏了状态本身，因此，非破坏性是量子传感器应重点考虑的方面之一。在进行实际检测时，可以考虑将量子传感器作为系统的一部分加以考虑，或者作为系统的扰动，将传感器与被测对象相互作用的哈密顿考虑在整个系统状态的演化之中。
实时性	实时性要求量子传感器的测量结果能够较好的与被测对象的当前状态相吻合，必要时能够对被测对象量子态演化进行跟踪。
灵敏性	量子传感器的主要功能是实现对微观对象被测量的变换，要求对象微小的变化也能够被捕捉。
稳定性	量子传感器在探测对象量子态时也可能引起对象或传感器本身状态的不稳定，解决的办法是引入环境工程的思想，考虑用冷却阱、低温保持器等方法加以保护。
多功能性	将较多的功能，如采样、处理、测量等集成在同一量子传感器上，并将合适的智能控制算法融入其中，设计出智能型的、多功能量子传感器。

1.4.3 量子传感器的市场应用

以英国为例，在传感器及相关设备领域的从业者已经超过 73000 人，对经济的年均贡献也超过 140 亿英镑。单单是一个传感器数据服务所衍生出来的价值就已经是天文数字了，所以整合全产业链的重要性也就不言自明了。

然而，有关量子传感器的想象力还不止于此：量子磁性传感器的发展将大幅降低磁脑成像的成本，有助于该项技术的推广；而用于测量重力的量子传感器将有望改变人们对传统地下勘测工作繁杂耗时的印象；即便在导航领域，往往导航卫星搜索不到的地区，就是量子传感器所提供的惯性导航的用武之地。

✧ 土木工程

地下勘测通常是极其昂贵和耗时的，但在建造新的基础设施时又是必要的，尤其是像高速铁路、核电站这种大型项目在开建之前。实际上有很多地质构造未探明的地下环境都存在诸如下水道、矿井和沉坑之类的危险。可现有的雷达、电子检测仪和磁力仪的性能并不能达到理想效果，超过地下几米的物体就很难被探测到了。

遇到这种情况，通常的解决方案就是使用重力感测技术，因为地下埋藏的任何物体的重力发生细微的变化都可以被记录下来并绘制成重力图。但传统重力仪的问题是读数不准确、耗时长且易于受到地面振动的影响。但如果用量子传感器来进行重力测量就会有明显的优势：速度更快、读数更精确、探测的更深且不受地面振动的影响。

✧ 自然灾害预防

山体滑坡灾害、地面坍塌和沉降、道路周报积水问题，自然灾害的出现对人民的生命财产安全造成了巨大的破坏，基于量子传感器快速扫描的特点，而这也使得常态化的检查成为了可能。

✧ 资源勘探

获取石油和天然气等自然资源的重点在于开采地点的确定，目前主流的勘探形式为地震探测，效果更佳，但更昂贵的重力测量方式只有在人们了解较少的地方才被采用。如今量子增强型 MEMS 传感器的出现就减少了设备调整的操作，使整个测量工作可以更快推进，连成本也降到了之前的十分之一。

✧ 交通运输和导航

交通运输越发展就越需要了解各种交通工具的准确位置信息及状况，卫星导航设备、雷达传感器、超声波传感器、光学传感器等都将逐渐成为标配。使用基于冷原子的量子传感器，导航系统不但可以将位置信息精确到厘米，还必须具备在诸如水下、地下和建筑群中等导航卫星触及不到的地方工作的能力。工作在太赫兹波段的传感器可以将道路评估的精度精确到毫米级。此外，最初为原子钟而开发的基于激光的微波源也可以提升机场雷达系统的工作范围和工作精度。

✧ 重力测量

光线测量并不适用于所有的成像工作，利用量子冷原子所开发的新型引力传感器和量子增强型 MEMS（微电子机械系统）技术在商业上也会有更重要的应用。

✧ 医疗健康

痴呆病：研究人员正在研究一种称为脑磁图描记术（MEG）的技术可用于早期诊断。但问题是该技术目前需要磁屏蔽室和液氦冷却操作，这使得技术推广变得异常昂贵。而量子磁力仪则可以很好地弥补这方面的缺陷，它灵敏度更高、几乎不需要冷却和与屏蔽，更关键的是它的成本更低。

癌症：一种名为微波断层成像的技术已应用于乳腺癌的早期检测多年，而量子传感器则有助于提高这种技术的灵敏度与显示分辨率。微波成像不会将身体直接暴露于电离辐射之下。基于金刚石的量子传感器也使得在原子层级上研究活体细胞内的温度和磁场成为了可能，这为医学研究提供了新的工具。

心脏疾病：目前正在开发中的磁感应断层摄影技术被视作可以诊断纤维性颤动并研究其形成机制的工具，量子磁力仪的出现会大大提升这一技术的应用效果，在成像临床应用、病患监测和手术规划等方面都会大有益处。

1.4.4 量子传感技术商业化前瞻

实验已经证明量子传感器在针对重力、旋转、电场和磁场等方面的灵敏度要远远超过常规技术。而我们努力的方向就是使它们更加耐用、便携。而在量子传感器商业化的过程中，有两点值得注意：

- 1) 在学术界和产业之间保持信息沟通顺畅；

2) 通过演示量子传感器如何解决现实世界中的问题，来强化商业供应链并建立市场信心。

根据英国国家量子技术计划的目标，英国政府应该建立起创新中心来测试量子传感器并开展相关的应用开发。一旦成形，这些设施将会为量子服务的开发提供肥沃的土壤，并形成一个深深植根于本区域的商业生态系统。对工程师进行这些新技术的相关培训也是十分必要的，不仅是为了他们能够与用户和市场开展互动，更重要的是清楚他们所面临的挑战。

基于量子传感技术可以实现对光、磁场、重力和角速度等诸多物理量的高精度传感测量，在科学研究和国防与经济建设等众多领域都具有广泛的应用前景。欧美发达国家在量子传感领域处于领先，中国在该领域的研究近年来努力追赶并逐渐缩小差距。

以量子陀螺仪、量子雷达、量子重力仪和量子磁强计等为代表的新型量子传感器，在国防建设和军事应用领域极具战略价值，受到世界各国政府和研究机构的重视，在解决工程化和实用化等问题后，有望在关系国家安全和国计民生的重点领域率先应用。据预测，健康监测、地质调查、安防设备中的重力和磁传感器等小应用程序中的量子传感器，针对高频金融交易中进行时间戳操作的更加精准的原子钟有望在 5 年内看到；针对汽车、建筑工程等更大量应用的量子传感器和量子导航手持设备在 5 到 10 年内可能会面世；基于引力传感器的重力成像设备，将量子传感器集成到移动客户端应用中的技术估计要 10 年以上达成。

1.5 量子成像和量子雷达

量子成像是基于量子涨落的非局域成像技术，也被称作“鬼成像”(Ghost Imaging, GI)，与传统成像相比，其具有非局域成像、单像素成像、无透镜成像等诸多优点，在高分辨率成像、非相干成像、恶劣条件下成像等方面具有广阔的应用前景。

1.5.1 量子成像技术

尽管，照相机和图片修改技术已经非常普遍，但大多数的照片拍摄仍受制于灯光的有无，且是二维的。但真实的世界应该是三维和多光谱的。探究量子特性能够帮助研发全新的成像设备，不仅超越当下最先进相机的性能，更能提供目前尚无法实现的、革命性的成像机制。通常说来，主要有两大类技术：

- 测量单光子的成像设备，例如单光子雪崩光电二极管(SPAD)探测器。基于 SPAD 阵列的相机能够在很短的曝光时间里快速探测到单光子，利用光子发射与接收的时间差能够实现三维成像，转角后物体的观测，以及普通相机无法工作的其他波段成像。
- 利用量子特性的成像系统，可以突破探测光线的限制。能够获取到更清晰的图像，并能将噪点降低到原来的极限之下。

1.5.2 重构看不到的世界

量子成像技术运用好，能让我们看到原先看不到的世界。

✧ 3D 图像

例如一项技术与全息摄影术具有相似之处，先以一束光穿过物体，并使这束光在物体背后与另一束完全相同但绕过目标物体的光交汇并重叠在一起，在两束光的相互作用下形成物体的 3D 图像。

✧ 转角后物体成像

一种利用光子超快飞行时间成像技术，能够让光“拐弯”的绝不仅仅是镜面反射，还有漫反射。最早是由麻省理工学院的科学家发明的，他们将一束超短的脉冲激光照射到地板上，就发生了漫反射并以球面传播到四面八方；当光传播到转角后的物体上，再次发生漫反射；一部分光到达相机观测视野内的地板上，并漫反射进入相机中，画出一条弧线。通过这条弧线以及光子到达的时间，我们就可以反向计算出物体的具体位置。

✧ 弱光强成像

用非相干 X 射线源，来实现以往只能利用相干 X 射线才能完成的、具有纳米分辨率的衍射成像。能避免云、雾和烟等使常规成像技术无能为力的气象条件的干扰，从而获得更为清晰的图像。

✧ 高分辨率图像

加州大学巴巴拉分校（UCSB）量子传感和成像研究组已经实现的技术。物理学家 Ania jayich 实验室的成员历时两年开发出一种全新的传感器技术，具有纳米尺度的空间分辨率和精致的敏感性。

✧ 鬼成像

鬼成像技术是指让一台高分辨率照相机为一个它本身并不能看到的物体成像，又称双光子成像(two-photon imaging) 或关联成像(correlated imaging) ,是一种利用双光子复合探测恢复待测物体空间信息的一种新型成像技术。

✧ 不可见的物体现形

传统相机捕捉的是物体反弹出去的光线。2009 年，格拉斯哥大学用一个分裂的激光束做实验，首次展现了这种“幽灵般的影像”。但科学家们说，这种使用两种不同颜色的激光束的新技术可以带来可视化领域技术的进步。

1.5.3 量子雷达技术

在军事和科学应用需求的牵引下，国内外在可见光、红外波段主被动强度关联遥感成像、微波关联成像雷达的研究方面竞争激烈，同时尝试将其应用于对地观测领域，以突破常规光学遥感和微波遥感的性能局限。

量子雷达是量子度量学的另一个重要研究方向，其本质是将光量子作为光频电磁波微观粒子对目标进行探测，利用它不同于常规雷达电磁波的物理特性，提升对目标的探测性能，同时提高雷达的抗干扰和抗欺骗能力。量子现象能够大幅度提高传感器灵敏度，促使量子传感器得到优先研发，如磁力计、光电探测器和密度计等。量子雷达比传统雷达的目标能见度更高，且量子旁瓣为射频隐身目标的探测提供了一种新方法。量子雷达具有优越的电子对抗性能，非常适合军事应用，因此受到各国军方的高度重视。

通过对量子不同物理特性的观测和测量，可以构成不同原理和形式的量子雷达。根据系统采用的量子效应的不同，可以把量子雷达分成三种基本类型，即发射非纠缠态光子的量子雷达、发射量子态光并与接收机中的光子纠缠的量子雷达、发射经典态光但使用量子光探测提升性能的量子雷达。

美国等军事大国和一些著名的研究结构非常重视量子雷达的研究，如美国国防高级研究局（DARPA）提出了“量子传感器计划（QSP）”；美国海军研究办公室（ONR）近期专门组织了一场研讨会，讨论量子雷达的科学性；美国海军实验室（NRL）的研究发现，即使考虑大气衰减，工作于 9GHz 的量子雷达理论上也可

以提高目标探测能力；荷兰莱顿大学的一个研究小组提出了一种机械装置方案，可利用量子点产生纠缠态的微波光子；西班牙 Pais Vasco 大学已经开发出多个工作在微波的单光子探测器的理论模型。

1.5.4 量子成像的市场空间

量子成像的最大市场或许来自于医疗成像领域。医用 X 光机目前在临床医学中被广泛使用，但是却将病患暴露在电离辐射之中。一项研究成果预测，到 2020 年，全球医疗诊断影像市场将达到 334 亿美元。

利用红外线成像也有众多的应用空间，例如，消防员能够透过浓烟看清火场，工程师可以检查天然气管道泄露，在安防领域可以被广泛采用。预计到 2022 年，单纯热成像的市场规模即可超过 112 亿美元。

能够直接三维成像的照相机也有无数的用途，到 2020 年 3D 成像市场预计可达 166 亿美元。

量子成像技术在弱光强环境下的安防和显微影像领域也会有巨大的市场。机载量子成像设备能够用于安全、军事、农业、石油、天然气和环境检测；军事领域包括转换测距等，水下成像，穿透浓烟迷雾成像，超视距成像等都能够拥有军用和民用价值。量子技术还能够廉价高效地进行地下工程的重力绘图，石油勘探和自然灾害防范，量子成像技术还能够增加量子安全通信系统的带宽。

1.6 量子化学应用

量子力学建立之后，很快就被应用到化学中来。1927 年，Heitler 和 London 用量子力学研究氢分子，提供了价键理论的理论基础，可以说从此就有了量子化学。近年来，由于新的实验成果不断涌现，理论方法日臻完善和计算技术的飞跃发展，使量子化学以更快的速度迅猛向前发展。目前量子化学的基本原理和方法已逐步深入化学学科的每一个分支领域中。从小分子体系到高分子化合物和生物大分子，在化学的各分支领域，量子化学的理论和计算都有许多重要的应用，量子化学不仅能提供分子结构和变化规律的微观知识，阐明物质结构和各种性质的关系，并且可以在此基础上进行分子设计（如光电材料的分子设计、药物分子设计等）。

1.6.1 量子化学基本原理和应用

现代化学学科正在经历从宏观到微观、从定性到定量、从静态到动态、从纯化学学科到各种边缘学科的发展，这一切都离不开量子化学的贡献。正如化学围绕分子结构展开研究，但研究分子结构的基础是原子结构理论，而原子结构理论的基础是氢原子薛定谔方程的解。目前量子化学还在飞速地发展，它在化学各个领域以及衍生的其他学科领域的应用层出不穷，日益变得广泛起来。

- ✧ 分子的平动、转动和振动
- ✧ 表象理论
- ✧ 电子自旋和角动量
- ✧ 多体问题和近似方法
- ✧ 原子结构
- ✧ 群论
- ✧ 价键理论

✧ 简单分子轨道理论

✧ 自洽场分子轨道理论

例如金属-碳簇由于在催化剂、超导材料、新电子材料、污染控制、化学示踪、蛋白质化学等领域的广阔应用前景而引起了人们极大的兴趣。近年来研究焦点更集中于过渡金属-碳簇上。例如量子化学家通过分子轨道计算，按化学键知识设计 Mo_2C_8 各种可能的几何构型并进行优化，从而得出最稳定构型。

✧ 后自洽场方法

例如通过研究 C_5H_5^+ 的各种异构体和反应 $\text{C}_3\text{H}_3^+ + \text{C}_2\text{H}_2 \rightarrow \text{C}_5\text{H}_5^+$ ，该反应对了解燃烧过程中煤烟的生成机理有重要意义。

✧ 半经验方法

✧ 密度矩阵理论

✧ 密度泛函理论 分子反应动力学

如果只是针对孤立分子而言，如果要与实验结果对比，只能对应真空或气相。然而很多化学反应都在溶剂中进行，很多性质（如光谱性质）的实验数据也都是在溶液中测得的，因此要把量子化学的计算结果与实验结果比较必须考虑溶剂效应。

氮氧化合物是大气污染物之一，而且它们对臭氧层具有重要的破坏作用，寻找有效消除或减少氮氧化合物的途径是燃烧化学和环境化学的重要课题，可采用反应动力学研究。

1.6.2 光电材料的分子设计

目前，在平板显示、手机、电视中液晶产品仍占整个市场的主要份额，这主要是因为液晶显示器有超薄、轻便、体积小、无辐射等优点，但它也有某些不足，主要问题是响应速度慢、被动发光（需要照明光源）、视角窄和工作温度范围窄等。

有机电致发光材料和器件(OLED: Organic Light Emitting Diode/Device)作为新一代显示技术随之应运而生。其基本结构是两电极间夹有机分子发光层（一般还应有空穴和电子传输层），在低于 10V 电压驱动下即可实现光的发射（高分子器件一般应低于 5V），发射光可从电极侧辐射出来，从而形成平板显示的基础。这种器件具有低开启电压、高亮度、高效率、快速响应、主动发光、视角宽、无辐射、可实现大平面显示及价格低廉等优点。

目前 OLED 的研究已成为国际科学前沿和热点领域，各国产业界已投入巨大人力、物力致力于这一研究领域。研究有机电致发光材料的分子电子结构，在了解分子电子结构与发光及载流子注入与传输性能关系的基础上，通过分子设计、探索改进材料的结构，实现对性质的调控，得到优良的多功能材料是进行理论研究的目标。

在理论研究方面，一般针对三大类分子进行：

1) 有机共轭化合物

通式为 $D-\pi-A$ 的有机共轭小分子是典型的非线性光学材料分子，可通过改变不同的 D （给电子基）和 A （吸电子基），以及不同的 π 骨架和链长来调节电子结构，从而对发光和载流子注入及传输性质进行调控。

2) 金属有机配合物

某些过渡金属有机配合物由于有强的自旋轨道耦合效应，有较高的三重态发光（即磷光）效率，从而可使器件的发光效率大大提高。

3) 高聚物和低聚物

共轭高聚物发光材料有良好的成膜性和可加工性，可通过旋涂、浇铸等方法制成大面积薄膜；有良好的黏附性、机械强度高、稳定；可改变和修饰其化学结构，调节其电子结构，从而对发光颜色和载流子注入及传输性能进行调控。目前实验上研究较多的明星高聚物为聚芴。

1.6.3 碳笼化学与物理

1985 年 10 月，美国 Rice 大学 Smalley 的研究小组 Kroto 等在实验上发现了一种新的单质碳形式，他们把激光产生的石墨蒸气通过一个高压的超声速喷嘴，得到了一系列新型稳定的碳原子簇，接着他们进行了质谱分析，发现 C_{60} 峰占绝对优势。他们认为这种 C_{60} 原子簇具有笼状结构，这一设想可比喻为当代的 Kekule 苯环结构猜想（1865 年），此后人们把这类由偶数 C 原子构成的封闭多面体称为 fullerene（碳笼）。

人们很早就知道碳有两种同素异形体：石墨和金刚石，碳笼就是碳的第三种同素异形体。

最初的研究表明， C_{60} 在大多数溶剂中溶解度很小，在空气中很稳定。量子化学理论研究指出， C_{60} 是稳定的闭壳层分子，所有成键轨道全充满电子，最高占据轨道和最低空轨道的能级差相当大，似乎难以进一步发生化学反应。

量子化学家一次次向碳笼分子的“稳定性”挑战，提出一个个新奇的设想，尝试用各种方法让碳笼分子实现各种各样的反应，从而开辟了一个全新的学科领域—碳笼化学。目前碳笼化学已有了蓬勃发展，其发展日新月异，处处体现了各类创新型思维的作用。

1996 年，诺贝尔化学奖授予 Cure R F, Kroto H W, Smalley R E 三位碳笼开创性研究者，这标志着碳笼化学的发展逐步走向成熟。各种各样的碳笼化合物的合成与表征使这个领域充满了生机和活力，而创新始终在碳笼化学的发展过程中起着首要的不可估量的作用。

1.6.4 含能材料在军事和航天的应用进展

含能材料作为分子的能量储存体，被广泛用于燃料、炸药、烟火剂，以高生成热（储能）及特殊电子结构为特征，构成独特体系。含能材料的研究不仅涉及高温高压极端条件，而且涉及激发态和快速化学过程，此外，反应过程所产生的中间体寿命极短，对实验研究提出巨大挑战。

因此理论与实验研究相融合，对于含能材料研究非常关键。量子化学由最初的解释实验现象，发展到预测未知体系性质，从而实现含能材料的高通量筛选，缩短研发周期和研究费用。

一种炸药化合物本质上就是亚稳定的。在高温高压下，输入相对较小的能量就能引发其极快（自传播）分解，产生气体产物（爆轰）。设计新型炸药，关键是在其两个内在矛盾的目标中寻求最佳平衡：高爆轰性能和避免意外引发的低敏感度。其指导方针包括：

- 分子应该是平面的，为了更好地填充和增加密度，提高由平行的晶层组成晶格的可能性，不易受致敏剪切应变的影响。
- 分子结构应有大的 N/C 比，为获得更高的生成焓和密度。
- 应该有一些氨基取代基。
- 如果在分子结构中碳原子数较少，可以提供更多的氧来氧化存在的碳和氢，同时稳定任何含多氮键的化合物。

为了研究模拟含能材料的分子间和分子内的相互作用，量子化学作为一个强有力的工具，能从微观尺度上显著、严格、系统地提高对引发反应过程的理解。目前的研究成果揭示了缺陷、形变、电子激发或带电状态在引发含能材料的化学分解中所发挥的作用必不可少。

人们不断寻求新的高能量密度材料（HEDM），使其储存的化学能明显多于目前使用的含能材料。随着介稳分子理论进展及其应用，如果实际制备并大规模使用这些分子，将对该类材料有高要求的国防、空间旅行等领域产生革命性的影响。

以量子化学不仅能提供分子结构和变化规律的微观知识，阐明物质结构和各种性质的关系，并且可以在此基础上进行分子设计（如光电材料的分子设计、药物分子设计等）。

美国国防工业和 NASA 大量研究自燃燃烧反应现象之后，肼和四氧化二氮的自燃点火机理引起广泛兴趣。为了帮助将来对这个重要推进剂体系的计算机模拟，可以进一步用高水平量子化学和统计理论计算，系统地研究潜在的链引发与链传递反应，阐明反应机理和提供大温度与压力范围内的反应速率常数。

1.7 量子钟

精确的“时间”是现代生活的基石。我们认为理所当然的技术，如手机，互联网和卫星导航系统，都依赖于原子钟提供的时间。

原子钟自 1967 年以来被用于国际计时，是目前最成熟的量子技术。英国在人类首个铯原子钟的开发中发挥了主导作用，但是在随后原子钟商业化的进程中被美国抢占了先机。近来，英国积极推动面向商业化的新一代原子钟技术，希望再次成为这一领域的领导者。

现在，原子钟的性能已经达到了前所未有的水平。最好的原子钟精度可以达到每 100 年误差只有几纳秒，并且突出小型化、便携性，成本也大大降低。这些发展开拓了全新的潜在应用和市场。此外，新一代原子钟还可以有效降低卫星定时信号中断带来的不便。

1.7.1 什么是原子钟？

所有时钟都需要一定规律的节奏来标记时间的流逝。这它可以来自机械时钟的钟摆或手表的石英晶体。而原子钟则使用原子来实现这一功能：原子以非常精确的频率吸收光或微波，并且这一频率可以被测量。该频率告诉我们在给定时间内完成了多少周期，而“周期”（光的振荡周期）正是我们需要的节奏：一个规则、可重复的计时单元。

包括早期产品在内的许多原子钟都工作在微波频率下。最近，可见光或紫外光频段的原子钟也成功面世。虽然微波频率下的技术在一直改进，较高频率段的原子钟具有提供更稳定时间信号的能力。

我们越来越依赖于 GPS 和其他全球卫星导航系统。然而，这些系统容易受到故障或信号中断的影响。错误的上传数据、各种空间信号的干扰，以及太阳风暴都会干扰整个系统。

全球卫星导航系统的重要功能是提供时间信号。从导航、通信，到金融交易，甚至电力供应系统，都依赖于卫星提供的时间。然而，这些系统的大多数都没有备份方案，卫星信号一旦中断就傻眼了。最现实的解决方案是在每个网络中嵌入原子钟。这也是英国《国家量子技术计划》、欧盟和美国竞相开发微型、低成本原子钟的主要驱动力。

1.7.2 原子钟商业应用

通信网络需要准确、稳定和可靠的时间源。信息通常被切割成很多部分，通过多个网络发送，最终在到达目的地时重新拼合在一起。如果不同网络不是以完全相同的速率传输数据，则数据容易丢失，或传输效率大打折扣。因此，相关国际标准规定了不同网络的传输速率差。

目前，使用卫星定时可以满足当前的标准。然而，为了增加数据传输的可靠性和提升传输效率，地面时钟的加入必不可少。

现在，移动通信网络的流量需求迅速增加，并且由于物联网中传感器的大量使用，互联网接入设备的数量呈指数增长。这对下一代 5G 网络及之后技术的定时和同步技术提出了更严格的要求。

电力传输网络也需要精确的定时，以确保不同电源在合并时保持同步，避免能量损耗。能源供应的安全、可靠和廉价都依赖于更加智能的基础设施。在智能电网中，精确的时序和同步变得比以往任何时候都更加重要。

金融市场同样需要精确的时间信号来同步交易系统，记录每次交易发生的时间。基于计算机交易的快速扩张，同步性和可溯性日益重要。所有交易用户都必须基于同一标准时间，才能有效防止不当交易，提供可靠的审计跟踪。

目前世界上最大的无线电望远镜是在建的“平方公里阵列射电望远镜”项目。建成之后，该望远镜将有达一百万个天线，使得天文学家能够以前所未有的分辨率观测宇宙。为了使望远镜阵列正常工作，所有信号源都必须同步在同一精确的本地时间下。

海底石油勘探也需要精确的时间。在实际操作中，船舶向海底发射声波，声音从不同的岩石层反射回来，被船舶底部的传感器网检测。通过记录反射波到达传感器的时间，我们可以建立岩石和沉积物的三维图片。

因此，图片的质量和精确度取决于时间的精度。卫星定时的信号不能穿透水，因此实践中通常使用石英晶体振荡器。然而，石英的定时精度随时间变化较大，并且容易受海床和海面温度差的影响。相比之下，微型原子钟可以在更广的温度范围下提供更稳定的定时。

各类空间应用的发展也离不开精准的时间。现在，通信和导航卫星的潜在市场十分巨大。根据欧洲委员会测算，伽利略全球导航卫星系统的开发预算为 24 亿欧元，而精确的时钟是这一导航系统的重要基础支撑。太空中的时钟需要在保持稳定精确的同时具备低功耗和体积小的特征，并且不需要频繁的校正。原子钟还可能推动深空导航的发展。利用飞船上稳定精确的时钟，航天器可以计算自身的时间和导航数据，省去了和地球双向数据链通的步骤，降低了任务成本，并提高了时间敏感性操纵（例如着陆或起飞）的能力。

军事方面，配有原子钟的雷达系统更加灵敏，更容易捕捉更小的目标。

1.7.3 量子间的国际备战

近年来，多个国家投入巨资启动量子计算研发。2016 年 10 月，美国国会举办听证会，讨论如何确保“美国在量子技术领域的领先地位”。IBM 投入 30 亿美元研发量子计算下一代芯片，微软公司与多所大学共建量子实验室。

欧盟从 2018 年开始，投入 10 亿欧元实施“量子旗舰”计划。英国在牛津大学等高校建立量子研究中心，投入约 2.5 亿美元培养人才。荷兰向代尔夫特理工大学投资 1.4 亿美元研究量子计算。

日本计划 10 年内在量子计算领域投资 3.6 亿美元。加拿大已投入 2.1 亿美元资助滑铁卢大学的量子研究。

澳大利亚政府、银行等出资 8300 万澳元在新南威尔士大学成立量子计算公司。

因为量子，世界主要科技国家以企业和科研机构为先导，均已“参战”。国际 IT 巨头近期集体“躁动”了。继 2017 年底 IBM 抢先发布“50 比特量子计算机样机”、英特尔于今年初发布“49 比特量子芯片”后，仍在研制的谷歌和微软的“新量子武器”，IT 巨头们急于抢占的是第一制高点：量子霸权。因为这是一场关乎未来的信息生产力之战。而量子霸权，正是新世界颠覆旧秩序的标志性转折点。

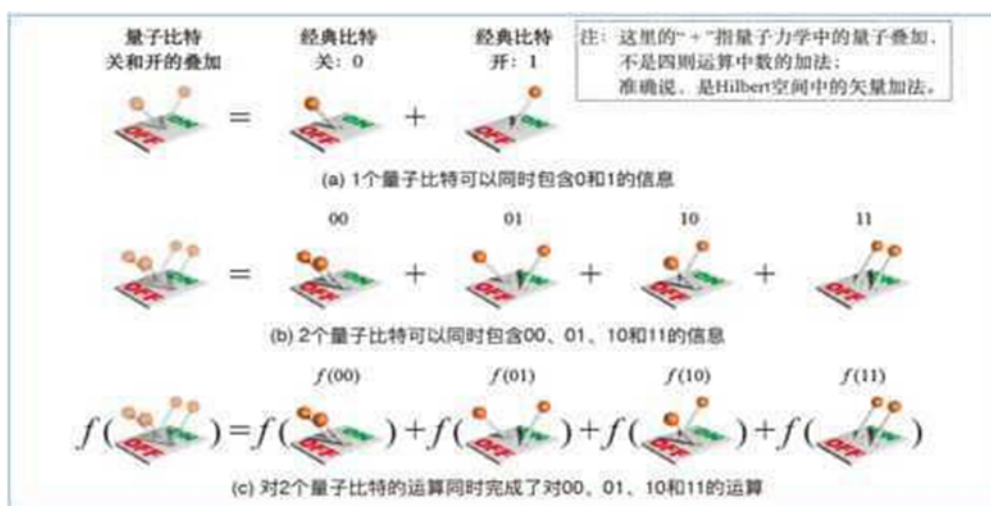


图 5 量子比特

因为量子，各国攻关量子计算机的战略已经明确，目前在超导、半导体、光量子、超冷原子等多条技术路线上推进。

决胜未来，国家行动计划

在中国《“十三五”国家科技创新规划》中，作为引领产业变革的颠覆性技术，量子计算机已被列入科技创新 2030 重大项目。未来 5 到 10 年是量子计算研究的窗口期和爆发期。如何统筹科研力量、深化产业协同。决胜关键在于资源布局与协同。因为量子计算机产业涉及硬件、软件、标准、工程技术、用户习惯等方面，需要政府支持、科研机构、企业合作乃至社会大众的关注。所以在量子计算机研究进入实用化、产业化的临界点，需要避免多个出现“量子热”造成的重复建设问题。

目前在产业化方面，已经有阿里巴巴、中船重工等公司与中科大量子科研团队开始合作，但无论是规模还是深度，与 IBM、谷歌等组建的“量子产学研联盟”都有较大差距。我国在相关科技领域研发投入，主要是依赖几大国有集团，民间资本投入极少。同样互为互联网公司，谷歌就能花几亿美元投资 SpaceX，而中国

的 BAT 则没有这方面的投入。如何吸引民间资本也参与量子信息技术产业投资，引入民间资本参与量子信息产业发展，激发竞争和活力。否则在参与国际竞争中，我们面临官方投入比拼美国官方+民间投入的局面，这是不利的。

2 什么是热链

目前在国际间，量子信息技术合作相对封闭，世界各国都在开始进行量子信息技术研究和商用备战；国家内部，传统企业与量子信息技术科研与实验机构的合作也存在壁垒。

这种合作的壁垒究其原因无非两点：

1、安全问题，这点大多出现在国家之间以及国家战略安全和民用之间；

2、利益问题，这点大多是商业公司与国有公司之间的矛盾。而这两点归结起来，就是缺乏互信、缺乏共识。因此，在量子技术应用领域建立一个跨国界的、可以保护参与者利益的、安全的量子应用技术合作联盟就是促进量子应用技术领域深度合作的关键，而这个联盟的核心就是共识机制。

量子技术领域内力量的整合对量子力学在各个层面普惠的意义是显而易见的。显而易见的是，这需要全社会共同积极参与的力量，而如何去团结这些力量，去达成更高和更加广泛的共识，是需要一个机制来引领的，由中本聪创造的点对点的电子交易系统，在货币数字化里完全抹去了中心化“第三方”的存在，在价值传递层面上，达成了广泛的共识机制，搅动了全球资本市场。这就是点对点背后的区块链技术，区块链技术不仅革新性地改变了金融市场的游戏规则，还引发了不少其他领域内的创新。未来，它将改变数据传输与存储的方式。完全可能会成为互联网的基础协议之一，所以要依赖区块链技术，在量子世界中与人们达成一种共识。

3 热链“区块链+量子技术”生态体系发展

3.1 从量子技术到区块链的哲学思考

道，可道，非常道；

名，可名，非常名；

无，名天地之始；

有，名万物之母。

-老子《道德经》

自然界最不可思议的事情是：自然界中竟然无时无刻不存在着各种各样的理性自治、普适永恒、精美绝伦的规律。用爱因斯坦(Einstein)的话概括就是：*The most incomprehensible thing about the world is that it is comprehensible*. 他认为：每一个严肃地从事科学事业的人都深信，宇宙定律中显示出一种精神，这种精神大大超越于人的精神，我们在它面前必须感到谦卑。

人们将这些亘古不变、万有普适的规律统称为“绝对真理”，是老子说的第一个“道”，是外在于人类认知的、客观的存在；但是，一旦人们以人类能够理解和接受的方式表述出来，成为人们创制的“可道”之“道”，就只能是相对真理，绝非“常道”之“道”。

自然科学第三基本公设是“自然规律理性自洽公设”，即自然规律全体必定是彻底理性、绝对自洽、全面和谐的。按照哥德尔不完备定理揭示：人类依据公设和概念构造的所有逻辑体系都不可能是绝对自洽和封闭的，**只能是开放的！人们总是力求和谐与自洽！**

烧脑费解的数学计算只是量子理论的外衣，更重要也更难的是理解它的灵魂---物理动机、物理观念、物理思想、物理图像、物理本质、物理逻辑、物理分析、物理结论、物理意义.....量子理论的物理属性极其丰富，除了常说的波粒二象性、不确定性、全同性这“老三性”之外，还有完备性、可观测性、内禀非线性、相干叠加性、纠缠性、逻辑自洽性、不可逆性、因果性、或然性、多粒子性、空间非定域性等。

2018 年美国当地时间 2 月 6 日，世界现役最强大重型运载火箭“猎鹰重型(Falcon Heavy)”从美国佛罗里达州带着一辆红色特斯拉电动跑车发射成功。火箭高 70 米，超过 20 层楼高，宽 12.2 米，标称近地轨道运力高达 63.8 吨。由 3 枚“猎鹰 9”火箭捆绑而成，拥有 27 个发动机。在历史上，只有上世纪的“土星 5 号”登月火箭的运力比“猎鹰重型”更强；在现役火箭中，全球排名第二、属于洛克希德马丁和波音公司成立的联合发射联盟的“德尔塔 4”重型火箭的运力只有“猎鹰重型”的不到一半。另外 SpaceX 公司的猎鹰 9 号一次发射约 6200 万美元，而联合发射联盟的官网的基本价格，Atlas 5 火箭，中文名宙宙神 5 火箭，基本价格 1.09 亿美元，而且这是基本价；目前人类在太空中建设的最大的生活舱是国际空间站，它质量为 370 吨，以目前火箭发射价格最低的 SpaceX 公司的猎鹰 9 号计算，需要约 17 次发射，按一次发射约 6200 万美元，所以国际空间站的最低发射成本是 10.5 亿美元，相当于非洲一些小国家一年的 GDP。而这仅仅是能满足 6~7 个人在距地面 400km 左右太空中生存的生活舱的发射成本。如果要达到万人的级别，这笔发射费就要到 10 万亿美元以上，目前年 GDP 能超过 10 万亿美元的国家只有美国和中国。另外我国重型火箭长征系列最多载重最大才是 25 吨，由此可以估算人们利用量子信息技术，探索人类更高文明这一巨大的挑战所需的花费和精力是多么的庞大。



图 4 “猎鹰重型 Falcon Heavy 火箭非主流的 27 台发动机

显而易见的是，这需要全社会共同积极参与的力量，而如何去团结这些力量，去达成更高和更加广泛的共识，是需要一个机制来引领的，由中本聪创造的点对点的电子交易系统，在货币数字化里完全抹去了中心化“第三方”的存在，在价值传递层面上，达成了广泛的共识机制，搅动了全球资本市场。这就是点对点背后的区块链技术，区块链技术不仅革新性地改变了金融市场的游戏规则，还引发了不少其他领域内的创

新。未来，它将改变数据传输与存储的方式。完全可能会成为互联网的基础协议之一，所以要依赖区块链技术，在量子世界中与人们达成一种共识。

如何引入民间社会力量参与，在这方面美国的 SpaceX（太空探索有限公司）进行了非常有意义的探索，走出了一条不一样的路，该公司雇佣了超过 5000 名员工，其组织形式和效率和美国官方机构截然不同。极大的增强了美国航天的力量。一方面国内拥有大把资金的各种资本到处在找项目，但是量子信息技术研究领域却没有投资渠道和项目，说明了我们在产学研的运作模式上有着极大的调整空间。

区块链技术的出现不但是一种技术应用的大革新，更是一种人与人合作的生产关系的变革。它让信任变的易得，让合作变得简单，为大规模的人之间的协作提供了良好的基础。热链基金会致力于通过区块链的思想来探索这样一种共识机制，去共建一个类似互联网的普惠大众的可行的量子技术应用的商业化的环境和生态体系，共享量子技术在民生领域商业化带来的现在和未来的市场价值。

热链的任务就是要通过共识机制、打破现有量子技术内部的壁垒，充分发挥现有能力，极致整合现有资源，为人们提供更高效、更有价值的服务，让量子科技更好地服务人们。

人类对于宇宙的探索是需要全人类的统一的共识来完成的，不是量子产业这一个行业能完成的，需要有一种模式来解决下面四个问题，让更多的人、更多的其他行业的机构进入量子领域，这样才能更有效地推动人类对量子科学的探索活动。

量子科学对于普通民众而言是遥不可及的，同样量子产业相对来说更是完全封闭的行业，准入门槛很高。究其原因，主要有四个原因：

- 一.市场属于早期，基础设施薄弱，量子产业应用的市场还属于早期阶段，不足以吸引其他力量进入；
- 二.成本高，没有一条低成本开展量子产业应用与探索的途径；
- 三.人才少，量子信息产业从业人员相对其他行业较少，导致量子技术转化存在较高壁垒。

四.周期长, 研究与实验周期长,民用商用转化还需时间，但是近年来，各国对量子科学技术商用的战略布局，人们越来越意识到量子是未来社会经济发展的方向，量子应用的市场也在不断的扩大，尤其是在民用领域上的市场不断增大。现在的商用市场已经有足够的优势去吸引社会其他的力量参与量子产业的建设和应用。热链基金会的任务就是解决成本高和人才少这两个问题，让更多人能参与量子信息产业的产学研过程。

但如果要使人类在量子比特世界的征程可持续发展，让人们宇宙的探索边界不断拓展，就必须激发出来自社会的广泛力量，这就需要更加开放协作的量子产业商业化的社会经济学模型。多年来，各个国家开展了大量的量子技术领域研究与探索，热链希望在解决量子商业化中的全民协作这个问题上，尽一点绵薄的力量。

如何解决成本高的问题

目前量子产业成本高的主要原因来自两个方面。一是量子研究工程与实验的成本，因为一切都还在实验室阶段，由于其技术尚未推广，世界范围内的商用成本还较高；二是量子产业基础设施薄弱，支持量子计算的芯片元是普通计算机芯片的百倍，相关终端设备的生产和试验设施的投入成本高，且资源相对垄断，使用成本高。这些问题都是很难解决的。但是量子科学的目标不是工程实现而是在民用领域大量的商业化，人们参与量子产业不仅仅是为了研究宇宙的秘密，而是为了寻求更美好的生活方式而开拓量子力学和其他学科交叉之后的技术成果的商业化道路，所以寻找更低成本地开展量子技术商业应用的方式，才是让更多的人参与

量子产业的有效途径。因此，打造基于热链的通证系统就是降低量子信息产业商用成本的最有效，最直接的手段。

如何解决人才少的问题

一直以来科研从业人员相对固定，非职业人员无法触碰到量子技术工程领域，主要原因是其技术有一定的专一性，且人员培养一是定向培养，二是周期长，没有经过专业训练的技术人员即使在自身领域有较高的成就也没有机会去为量子技术研究出一份力。这就是量子产业技术封闭的原因。因此，让更多更好的科研技术人员能够参与到量子力学和其他交叉学科领域的探索，不但能直接增加量子科研领域的人才数量，还可以将其他领域优秀的技术能力注入量子技术产业，形成极大的增量效益。因此，降低量子技术产业的准入门槛和提升量子技术研究的技术水平，就成了解决人才少的问题最重要的手段，其主要方式有：

- 1.降低准入门槛：去繁就简，让参与项目对开发者的要求降到最低；增加参与维度，从操作系统、硬件系统等多个方面吸引人才；
- 2.在高等教育中大力普及量子力学和量子交叉学科基础，增加人才储备；
- 3.推广和科普量子技术，提高大众对量子技术产业工程、量子技术商业化的认知，增加潜在人才储备，同时引导公众资源投入量子产业。

3.2 热链生态圈-量子技术商业化产学研联盟

热链（HeatChain）是面向量子技术应用产业的自主区块链底层，并构建其上的以量子技术资产交易中心为核心的业务体系，来克服严重的安全+利益壁垒的中心化治理思想，尤其是在量子技术早期阶段，由于落后的量子产业底层基础设施、造就的量子技术商业化的难度，由此构建的分布式量子产业经济生态。

整个热链生态体系是开放的！如同热力学第二定律（熵增定律）表明，封闭系统的熵是一直增加的，如果不增加有效能量，那么最终系统就会熵死。

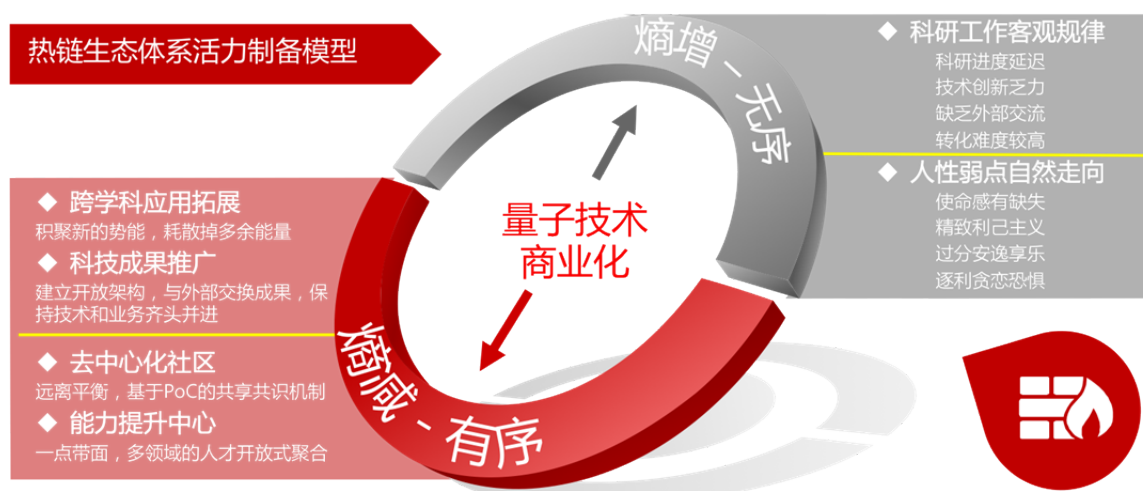


图5 热链生态体系活力制备模型

第二次量子革命即将来临，全新的量子技术正从实验室走出来，这将使传感、通讯、量子医疗，信息处理等领域获得前所未有的跨越式发展。但最大的挑战还是在于如何将技术概念变为原型，以及如何成功将原型进行商业化。

因此，在量子信息技术应用领域建立一个跨国界的、可以保护参与者利益的、安全的量子应用技术合作联盟就是促进量子信息应用技术领域深度合作的关键，而这个联盟的核心就是共识机制。要达成量子技术共识，需要打破现有阻碍共识达成的壁垒，这个壁垒来自两个方面：

1.安全问题。量子技术涉及信息安全、国家安全等问题；

安全共识首先需要确定的是热链的范畴在于商业化的民用领域，不涉及政府、军事国防领域。热链期待整合的是愿意共建一个类似互联网的普惠大众的可信的量子技术应用的商业化的环境。

2.利益问题。技术分享没有好的合作共赢模式导致的成果变现极度困难。利益共识是量子信息技术商业化存在的最重要共识壁垒。

量子技术、资源分享缺乏有效的合作共赢模式而导致各个经济体之间的合作不畅。这主要体现在量子技术研究机构对新兴商用公司之间的技术封锁。量子技术科研机构一方面由于发展较早就得到了国家的倾力支持，以至于他们在技术、工程和实验能力、基础设施及不可再生资源上有着明显的优势。

而另一方面，新兴的商用公司看到量子技术在民用领域的普惠性，则更具活力、更贴近市场需求。由于无法保障技术持有方分享技术成果后的利益，现有的专利系统、技术保护体系及合同协议模式过于繁琐和低效，导致技术、资源分享不畅，从而导致最贴近市场需求的公司得不到必需的技术及资源去服务市场，最终结果就是量子信息技术应用的服务效能变差。

区块链的技术发展，也从某些方面体现着这种属性，例如去中心化的分布式记账行为在空间上是非定域的；去信任的共识机制是逻辑自洽的；交易数据是可观测的、不可逆的；智能合约需要是图灵完备的；集体维护的分布式账本是全同的……毫无疑问区块链+量子技术应用这是人类的科技进步和突破。人类出现至今已有近 10 万年的历史，10 万年里人类从蛮荒走到了现代文明，从几十人的部落到几十亿人的世界村，这 10 万年中，人类探索未知和文明脚步从未停止，而支撑这种探索的力量来自于大多数人的共识。不同的共识集合了不同数量的人类群体，解决了不同难度等级的问题。而当面对人类文明的量子产业化这一发展问题的时候，如何探索一种共识来集合全人类的力量就成了一个需要解决的问题。

同样的，要打破这一共识壁垒，可以利用区块链技术打造的通证系统。通证（俗称代币），即可流通的数字加密权益证明。它的高效的流通性，使通证系统可以保证技术分享的简约化，同时由于通证本身数目的确定性，技术分享带来的行业发展可以直接由通证的价值增长来体现，这也保障了量子技术分享方的分享技术的利益，从而从根本上打破利益分配带来的共识壁垒，可以在量子力学+交叉学科研究内部，形成共识。

热链基金会以“区块链+量子技术”为契机，以量子思维的基因，以量子技术商业化协同为使命，建立的社会经济学模型，就是要利用热链的通证系统建立量子产业领域的生态链，让每一位参与者和贡献者都获得公平的回报，通过这种社会经济模型吸引更多的资源体参与量子技术领域的产学研建设，达到政府、科研、转化、投资之间的和谐。热链的生态圈建设目标是，推动量子技术研究机构跨学科应用拓展，与国内和国际企业和投资机构间加强协调，建立伙伴关系。除此之外，热链还会建立创新中心，联合学术界和工业界，让量子技术商业化。能够促进量子技术产业的发展，使其成为中国各行各业科技进步的底层横向支撑层，将是

整个联盟持之以恆的奋斗目标。



图 6 热链生态体系规划

因此，热链基金委员会将谋求广泛合作，在专家委员会的评审机制下，与具有领先地位的科研机构合作，制定各类科研项目发展计划、开放实验室计划；与政府科技管理机构、产业联盟等合作，建立量子技术资产交易平台和国际技术合作服务平台；与科技转化企业、投资机构等合作建立投融资对接平台。

热链社区还将搭建一系列的公众服务平台和 IT 系统，包括热链钱包、数字资产交易中心、量子技术产品首发平台和电子商城、量子技术商业观察媒体和热链社区系统。对量子信息技术领域的初创公司，热链基金会会提供资金、技术、资源、人员等各方面的支持，同时推广热链及热链通证系统，促进其快速成长、更及时地提供更贴近市场需求的服务和产品，推动技术成果走出实验室，面向市场加强科技转化，让量子技术产品走向更广泛的应用领域，让成熟产品真正惠及各行各业、千家万户。

3.3 量子技术商业化产业促进平台

热链区块链底层是一个授权的联盟链，是一条针对量子技术应用产业特别设计的底层区块链网络，它开放、可扩展，能够基于热链生长出很多可能。它将会开放给所有有志于从事量子产业区块链应用开发的开发者，帮助他们基于热链及热点搭建不同场景下的应用，在物理网络的基础上推出热链通证，秉持开放的心态，促进更多的量子技术分布式应用接入到热链中，共同进步，集约发展。产业化促进平台

✧ 量子技术科技发展计划

热链诞生的本质就是为了促进量子技术的科学进步，利用区块链技术在商业化进程中发挥力所能及的作用。热链发行的通证中，最大的单笔用途就是设置量子技术科技发展计划，由量子技术专家委员会针对科研项目进行评估和资金扶持。

专家委员会制定年度科技发展计划，包括对量子技术前瞻性技术研究和技术交叉融合创新项目进行扶持、设置热链科技奖金、设置热链人才培养奖学金等。

◇ 量子技术开放实验室计划

量子技术开放实验室是量子技术应用领域的一揽子资源开放共享平台，是以推动“量子技术商业化”为目标的、非营利的开放合作与资源共享服务平台。

目前量子技术相关的仪器设备价格高昂，跨学科科研时往往因为经费问题导致其他学科难以开展工作，而量子技术的科研人员也容易因为缺乏应用场景导致后续科研方向性困惑。因此热链计划与全国重点高校开展合作共建开放实验室计划，目标是建立 10-20 座联合实验室，由热链负责提供仪器设备和基本的运作经费，由量子技术专家委员会甄选具有国内领先科研和指导服务能力的院校，由合作高校提供场地、专家和日常运营管理团队，并开放给其他院系、高校和企业使用。每个开放实验室结合落地高校的科研实力，聚焦一项量子技术的应用领域，例如通信、计算、传感、光学、化学等等。

量子技术开放实验室本着“融合、开放、合作、共赢”的理念，以“联合优势单位、释放优质资源、创新人才培养、助推跨界整合”为目标宗旨，以“释放优质资源和创新人才培养”为核心，助推量子技术及辐射的产业应用发展。

量子技术开放实验室系统规划仪器、数据、专家和研究四类资源的开放共享，并通过建立分实验室推动各类资源的开放共享，每个共建实验室作为各商业应用领域产业发展的聚集区和辐射中心，将整合全国优质资源支持和服务该区域、该领域产业的发展，构建可持续发展的生态格局。除了硬件设施以外，还将建立专用数据中心、公共数据中心。每个共建实验室由高校科研人员负责教学试验计划拟定、申请、安排和评审工作。

量子技术开放实验室的收费项目将接受热链的通证作为支付手段，经费拨付也将以通证为主、法币为辅的方式进行。

◇ 量子技术资产交易平台

量子技术资产交易平台，既是基于热链（HeatChain）搭建的量子技术商业化的核心基础应用，同时又是热链体系本身不可或缺的一部分，它是热链上的独特存在，它使得热链本身具备独特的竞争优势和价值。打造卓越的量子及衍生技术专利与科技服务交易平台，为科技创新和商业化应用提供优质的服务。量子技术资产交易平台将与中国生产力促进中心协会、亚欧国际科技评价中心开展深入合作。数据层面将与中国科技部及国际合作组织等数据库中心进行对接。交易平台的核心价值在于：

- ◇ 能够实现优质量子技术资产数字证券化交易；
- ◇ 基于热链成为一个重要的虚拟场所和纽带，将行业上下游连接在一起；
- ◇ 基于热链及其开放特性，有机会做到融入研究与生产或其他类似消费场景的投资，从而将优质量子信息技术资产和更大范围、更精准、更专业的投资者连接在一起；

以区块链技术、智能合约等为基础，实现量子技术资产权属的海量切割、流转过程追溯、收益分红管理等，使得量子技术资产投资变得小额化、简约化；

这些带来的好处是：打破技术安全+利益的壁垒，使得量子技术更早变现、项目方更早获益；更加方便利用大众投资，使优质量子技术资产更好的商业化；将闲散资金和量子资产更好结合，利于更长期、多元的量子技术商业化。而这些最终都将帮助热链团队，实现一直期待的构建的量子资产的价值链。

技术资产交易平台服务能力围绕“静动促”三个关键字展开：第一，“静”的方面特指资源中心，系统聚合科研院校、领军专家、科技专利、科技成果、实验室、仪器设备、各级政府及政策、科技转化企业、投资机构、服务机构等，方便供需双方的信息展示和相互考察；第二，“动”的方面特指快速对接通道，例如科研机构和转化企业可以发布融资需求，便于政府招商和投资机构对接；再如企业张榜科研需求，有实力的科研机构、专家等可以揭榜承接；还有科技成果转移，引入基于大数据的科技成果自动评价体系与专家评价体系，便于技术先进性评估和交易价格评估。第三，“促”的方面特指技术交易的线上线下展会与对接会、量子技术成果转化项目的投融资路演活动、量子技术新产品路演活动、专利及科技成果的竞价凑合平台等。

量子技术资产将发布到热链的侧链中。技术资产交易中心的在线交易部分支持热链通证。

✧ 量子技术国际合作服务平台

量子技术国际合作服务平台是推动国际间量子技术及衍生科技成果跨国合作的促进平台，与中国国际技术转移中心和亚洲产业科技创新联盟共同建设 IT 平台；建设及运营管理工作与技术资产交易平台整合。

通过国际间的科技合作协作网络，提供科研及合作国家政府解读等科技情报服务、专利及科技成果的对接服务、专利及科技成果的技术评估和交易价格评估服务、技术推广项目对接服务等。

✧ 投融资平台

热链基金会的执行机构将与中国创新投资机构密切合作，方便科技转化项目的人才、市场和资本的对接服务。投融资平台将一如既往的关注量子技术转化项目的品质，倾尽平台渠道，为投资机构推荐精品项目，为转化项目直接向合适的投资人进行投递，并定期举行线下投融资对接会。

投融资平台也是量子技术产业化项目众筹的辅导机构，是热链中各类去中心化应用的拓展机构。例如未来某个量子技术转化项目在获得专业投资机构领投之后，可以面向热链社区中的私人投资者发起基金跟投，此时投资基金份额即可按照 DApp(Decentralized ◇Application)模式发行到区块链上，可以利用热链通证融资，并且运行在热链记账节点之上。

如果某项量子应用技术已经非常成熟，可以进入产品生产和销售阶段，则可以利用热链发起众筹，其他企业、研究机构或者个人以热链通证进行认购，达到预期的众筹目标即可正式启动生产和配送工作。

3.3.1 社区基础服务平台

✧ 热链钱包

热链钱包是存储热链通证的手机 App，基于热链开发的 DApp 和在量子数字资产交易所交易的其他 Token，可以获得热链钱包的支持。钱包基于加密技术实现，注册用户生成每种资产的接收地址，并通过私人密钥管理个人加密钱包。

钱包支持各品种资产的查询、转账和收账功能，需要使用备份副本和安全访问密码，防止黑客攻击，规避密钥管理不善对用户的财产损失。

✧ 量子数字资产交易中心

数字资产交易中心是一个方便量子技术转化项目进行融资活动的平台，也是量子技术爱好者交流和价值发现的平台。交易中心聚焦于基于热链开发的，或者与量子技术资产相关的其他区块链场外交易。交易中心不直接参与热链通证的买卖，而是面向以热链通证计价的各类数字资产。

为了切实保护交易中心投资者的利益，交易品种必须有各类权益作为背书，无任何法律意义上背书的数字货币将不允许纳入交易范围。

✧ 量子技术产品首发平台及电子商城

平台采取 B2B2C 模式，打造多商户的量子技术产品的首发平台和电子商城。量子技术产品源于热链社区关注的各类量子技术转化机构生产的仪器设备、网络设备、模拟器、量子算法相关软件应用等，或者是产品研发过程中充分利用了量子技术进行模拟计算、仿真、转换等的消费级产品，所有商品都必须令人信服地使用到量子技术。

电子商城支持热链通证作为全部或者部分支付手段。系统建设量子技术产品首发机制，如果某项新产品在商城率先独家三个月，平台将安排该产品的线上线下路演活动，并在电子商城中分配专门的促销资源。

电子商城支持销售众筹模式，商家可以发起预售众筹，消费者进行在线订购。在众筹期间消费者的资金将被暂时冻结，如果众筹目标不满足则全额退还；如果目标达成，再由商家进行产品生产和配送工作。

✧ 量子技术商业观察媒体

专注于量子技术民用化、商业化领域的各类专家访谈，科技成果展示、科研活动进展、量子技术知识科普、热链重要事项发布等。

媒体特向量子技术各领域的科研专家和企业进行约稿，并建立类似于维基百科的审核机制，确保具有专业性的文章才能进行发布。把《量子技术商业观察》打造成量子技术促进、科普的新闻来源，并开放给其他合作媒体转发，防范伪科学。

投稿者和审稿者将获得一定的通证作为工作酬谢。

✧ 热链社区

热链社区是基于量子技术商业化产学研联盟的价值共享平台。用户可以通过浏览、推荐、转发、打赏等活动深入了解量子技术及相关应用，并向更多人群介绍科学家们的丰盛研究成果。

热链基金会为热链社区用户分配一批通证，作为激励社区活跃度和知识传播的动力。

3.3.2 热链分布式应用 DAPP

热链分布式应用(Decentralized Applications, DApp)是运行在热链区块链网络之上的，是热链生态体系上衍生的各种分布式应用实例。与其他区块链 DApp 定义所不同的是，热链分布式应用具有如下特征：

- 1) 所有分布式应用必须运行在热链联盟节点所组成的网络节点上；
- 2) 分布式应用需要使用热链通证作为 Gas 费用；
- 3) 分布式应用使用的智能合约必须由授权的开发方使用私钥进行签名才能发布，智能合约必须经过全节点审核并达成共识后才能生效或者升级；
- 4) 分布式应用的程序开源，数据加密保存在物理网络上；

3.3.3 授权的联盟区块链网络

热链是一个授权的联盟链，整个区块链服务的记账节点主要面向科研院所、合作实验室、热链分布式应用开发者、科技转化企业和投资机构等开放。区块链服务有三个关键部分组成：

➤ 点对点 P2P 协议

点对点协议运用的是谷歌远程过程调用协议，其功能包括双向流、流控制、在单一连接下的多路复用要求等，能够为对等节点采用的信息提供由点对点到多路传送的定义。

➤ 分布式账本服务

数据结构经过优化能够有效有效维护众参与者重复的整体状态。大型文件存储在区块链账本之外的侧链上。

➤ 共识机制

共识机制使用实用拜占庭容错算法，其在容错性与扩展性方面都有强大优势。采用一种按照贡献度的协商机制轮流获得记账权，不采用 PoW 等挖矿机制，以便把宝贵的计算资源用于科研，而不是白白浪费掉。

3.4 热链区块链的技术架构

热链追求政府、科研、转化、投资之间的和谐，**打造量子技术商业化的产学研联盟链**；因此区块链系统的组网、智能合约的发布均遵循此理念进行。

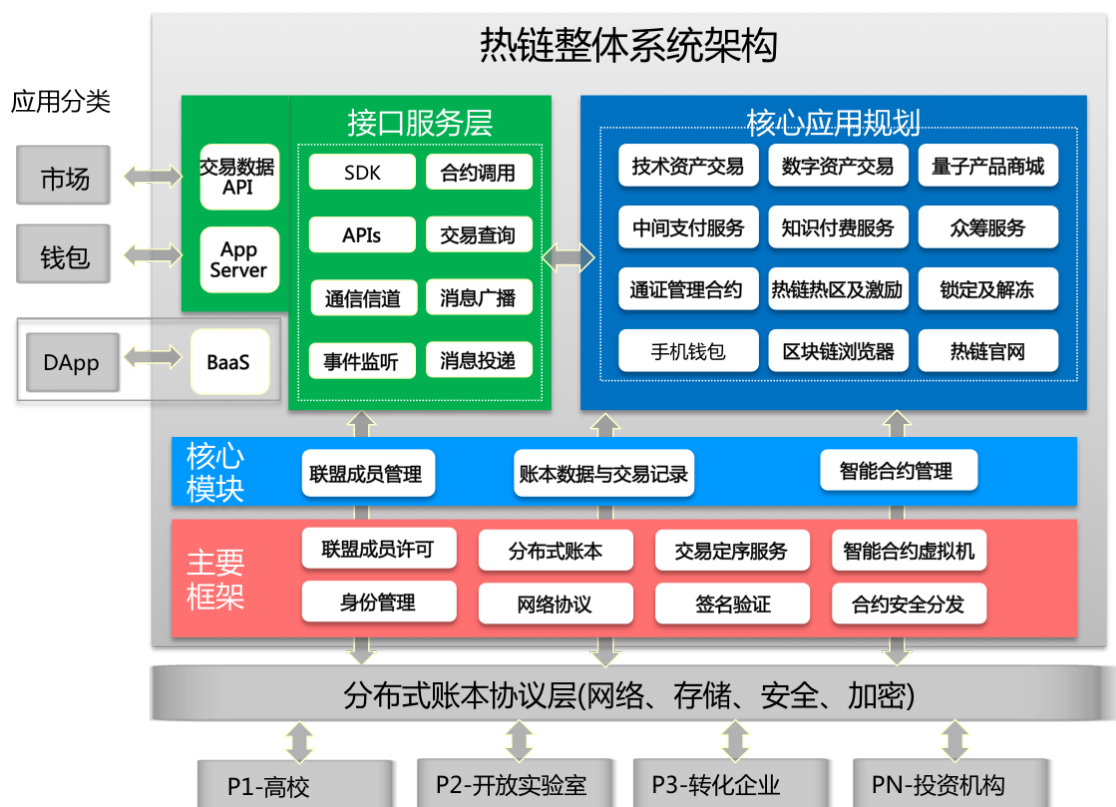


图 7 热链整体系统架构规划图

上图规划的物理设备、核心模块、接口层和应用层的开发部署工作，需要由热链基金会向开发者拨付并进入流通环节以后才能全面启动。热链的底层架构将基于成熟的开源平台进一步研发，技术选型将以超级账本 HyperLedger 为基础，并借鉴以太坊的相关共识机制和区块创建激励机制。热链的整体系统架构从底层开始到顶层应用，分为如下部分：

3.4.1 协议层

由量子技术商业化产学研联盟共同提供设备和计算能力，每个节点独立存储全网区块链交易数据和本地账本最新状态数据，并按照低信任度的方式达成共识和数据同步，节点间的通信基于点对点协议实现。

3.4.2 主要能力框架层

联盟成员节点必须经过热链执行委员会评审才能接入网络中，并能够对节点身份进行管理。政府或监管机构也可以接入进行审计。来自于应用的交易请求数据广播到各个验证节点进行签名，并根据时间戳进行交易记录定序后通知各个网络节点记账到本地；智能合约的发布过程也是一种交易类型，遵循类似的签名验证工作，不同分布式应用的智能合约可以运行在安全的沙盒中，从而规避冲突。

3.4.3 接口服务层

系统提供相关 SDK 和 API，供公共服务平台进行调用；支持 BaaS(BlockChina as a Service)模式，可以将系统基础能力和热链通证服务，便于第三方开发者快速开发、测试和部署分布式应用到热链基础平台上。

系统提供基础的通信信道管理机制、事件监听服务和消息管理机制，保障应用层和区块链系统的对接。

3.4.4 核心应用层

按照热链生态圈的业务体系规划，热链执行机构将开发部署一系列的应用系统，将相关服务通过互联网及移动互联网提供给所有社区成员。

应用层面向第三方开发者开放，以便将各类量子技术转化的需求形成单独的分布式 App。优质应用定义的加密资产还可以进一步得到热链钱包和数字资产交易中心的支持。

3.4.5 热链通证的过渡方案

热链团队会自筹资金，先基于以太坊公链发行热链通证热点，早期热链的参与者可更早进行热点的交易，而不必等到热链自有区块链平台正式上线。热链正式上线后，我们会将热点向热链迁移，具体迁移方案会在热链主网上线前详细说明。

4 热链 TOKEN 发行重要事项探讨.热链的通证系统---量子信息技术资产的代币机制

4.1 热链的通证系统---量子信息技术资产的代币机制

热点 HFR 是热链的原生数字资产。它可以衡量和体现热链上的数字经济行为，同时也是价值流通的媒介。热点既代表了热链的使用权也代表了所有权。使用热链或热链上的应用可能需要支付一定数额的热点，体现了使用权；持有热点，即代表拥有热链的一部分，相当于持有热链的股权，能够参与到热链治理的各个环节，体现了所有权。

利用区块链世界的通证（Token）理念，实现量子技术资产证券化，是交易中心的一个重要策略，也是一个核心机制。另一个重要的策略是，热点 HFR 作为热链 HeatChain 的价值流通媒介，所有量子技术产业所发行的代币都是面向热点的。换句话说，所有量子技术资产的代币在募集的过程中，筹集的都是热点 HFR，同时，在交易中心针对量子资产通证进行交易的时候使用的也是热点。落地到细节，主要涉及如下几方面内容：

量子产业资产的盘点及权属边界的清楚界定，这一工作主要在区块链数字资产交易中心登陆审核环节完成，它的本质是把一份量子技术商业化过程中变成一个拥有确定价值边界的量子数字资产的过程；

通证体系设计及项目上线准备，如上所述，这一工作由专家及科研机构组成的项目服务商业委员会，会同具体的量子技术产业项目方共同完成，我们可以把这一过程看做是制作特定量子资产数字证券化的具体方案。当然，不同的量子资产可能会有不同的方案；

热链通证的认购和交易，特定的量子资产通证，对应着特定量子资产的价值和权益，拥有通证即拥有这些价值和权益，拥有因此而来的、可能的未来收益；

流通媒介热点 HFR 的主要用途是完成热链上的各种交易、支付记账手续费及部分有偿应用的使用费，如量子技术成果产权登记、量子技术资产交易等。

另外，热点还对应了一块非常重要的额外价值。在热点上线交易后，热链基金会将会基于交易市场上的热点价格，在全国挑选有巨大潜力获得商业成功的量子科技产业，购买其产权。一方面，这些产权将直接成为热点的价值基础，拥有热点，即代表拥有这些量子科技资产相对应比例的权益；另一方面，这些优质产权将成为热链上诸多应用的商业种子，尤其是我们正着重规划的量子技术资产交易中心。

这些量子技术的产品数量预计在 5~10 个左右，期望涵盖拥有较多消费者的方向，并主要侧重计算机、手机通信设备、新能源电池、量子新材料等几个领域。我们期待这些被赋予量子信息技术的产品在未来能够在商业上获得可观的回报，也期望通过这些量子产品的成功，最终回报给热链的早期投资者。对于这些量子产品，热链团队将尽力扶持，提供一系列产品孵化服务，挖掘它们在不同领域和产业方向的价值。

长期来看，随着发展与成熟，热链必将逐步支撑起一个以热点为流通媒介的量子信息产业价值体系，包含交易支付结算、产权金融和技术产权资产交易与转移等。这给热点的价值基础带来了更大的想象空间。

热点的获取，热点不可或缺，它是认购和交易量子信息资产的媒介，关于热点的获取方法，请参考白皮书中“分配与发行”部分的内容。

4.1.1 热点的分配与发行

如上所述，热链 HeatChain 发行热点 HFR，发行总量 30 亿，初次生成 24 亿。剩余 6 亿，依照发行曲线，通过生态激励机制进行分配，伴随着数据的积累、生态的生长繁荣逐渐增多，直至预计 20 年后达到 6 亿。

热点分配方案

- 1、8%的通证 HFR（2.4 亿）将在初始阶段分配给参与者和热链早期应用的开发者；
- 2、15%的通证 HFR（4.5 亿）分配给热链创始团队和极早期贡献者，他们是为热链的早期发展提供资源和技术的支持者，支付热点作为回报；
- 3、30%的通证 HFR（9 亿）分配给国家顶级量子信息研究机构 and 高校及其他被授权机构；用于开放实验室建设、科技支持计划、科技奖励和奖学金、运作经费等。
- 4、2%的 HFR（0 亿）分配给社区，主要用于奖励热链社区的卓越贡献者；
- 5、15%的 HFR（4.5 亿）通过生态激励产生，主要用于奖励那些对于热链生态繁荣，
- 6、10%的 HFR（3 亿）作为后期热链的技术开发及运营维护；
- 7、5%的 HFR（1.5 亿）作为私募用，筹措科技计划、产业化和社区平台建设所需的运营经费；
- 8、15%的 HFR（4.5 亿）作为商业拓展用，主要用于挂牌交易或其他产权合作所需费用；用于量子技术资产交易平台、国际技术合作服务平台、投融资服务平台、数字资产交易所的合作、系统建设、运营等。
- 9、热点 HFR 计划在条件成熟时，登陆数字货币交易中心，开放交易。

4.2 量子商业化和收益回报体系

这是热链业务模型的最后一环，包括两个部分：商业化团队及收益回报机制。收益回报机制，是依靠基于热链的智能合约来实现的，这些智能合约在热链的准备阶段就已经设计完成并同步发布了。

商业化团队，属于热链业务体系，他们主要做两件事情：第一、监督所有登陆交易中心的量子技术资产的孵化交易，保护生态和投资人的利益；第二、推动、挖掘、服务于量子技术产业的商业化。以此构建一个良好的商业化和收益回报体系。

- 产业基础平台以通证记账的收入部分

热链基金会支持的基础服务平台执行企业，将会提供计算机作为区块链全节点进行记账并获取记账手续费，手续费完全以通证方式收取。这种情况下，每个季度将手续费收入的 10%，转移至销毁账户进行销毁。

回收代币销毁账户为：**not-valid-account**，这是一个初始账户，没有任何人可以掌握其私钥并动用账户里的资产。整个销毁过程的记录可以通过区块链浏览器查询。

● 产业平台现金利润方面

由热链基金会 100%控股的产业平台，有些会产生现金收入并最终形成企业利润。该平台每年核算税后利润，并将利润的 20%-30%拿出来，在次年度开始，持续在热链通证挂牌交易的二级市场上公开回购。

当然回购行为也分为两种：

1) 回购后销毁

回购后销毁有助于减少二级市场上的通证流通量，从而推动价格上升，并继而对其他持有通证的投资者带来更高的投资回报。销毁的通证，应以公募或私募过程中，募集的通证数量为最高限度，超出后停止回购销毁操作。

2) 回购后赠送给持币人

当回购后的通证不再销毁时，则按照一定的规则统计，例如某个截止日前用户持有通证天超过 90 天的钱包地址，按照通证地址的持币金额进行平均分配。

这样，将产业平台收益能够以回购再赠送的方式反哺给投资者，从而使通证有切实的收益。

目前，产业平台收益不适合用法币方式分红给投资者，原因是区块链中并没有记录用户的银行账户，无法现金转账给用户。

5 热链（HEATCHAIN）的治理机制

5.1 治理机制

热链是一个去中心化的国际性区块链社区，将在海外设立热链基金会来保证热链社区的管理、运作，以及所募集资金的管理和安全。热链基金会的组织架构将由热链社区大会，热链基金自治委员会和执行委员会组成。详细细则见“热链基金委员会章程”。

热链社区大会是热链社区的最高权力机构，由全部热链持有者组成，所有的持有者都能够通过社区大会行使自己的投票权，参与社区重大事项决策。

热链基金执行委员会对社区大会负责，负责对执行委员会行使管理和监督的职能。每两年根据所持代币的数量和币龄进行换届。

自治委员会对执行委员会负责，负责热链社区的正常运营和维护，下辖技术开发组、商务运营组、财务管理及风险控制组以及品质把控组团，每个组团负责相对应业务的实际工作。

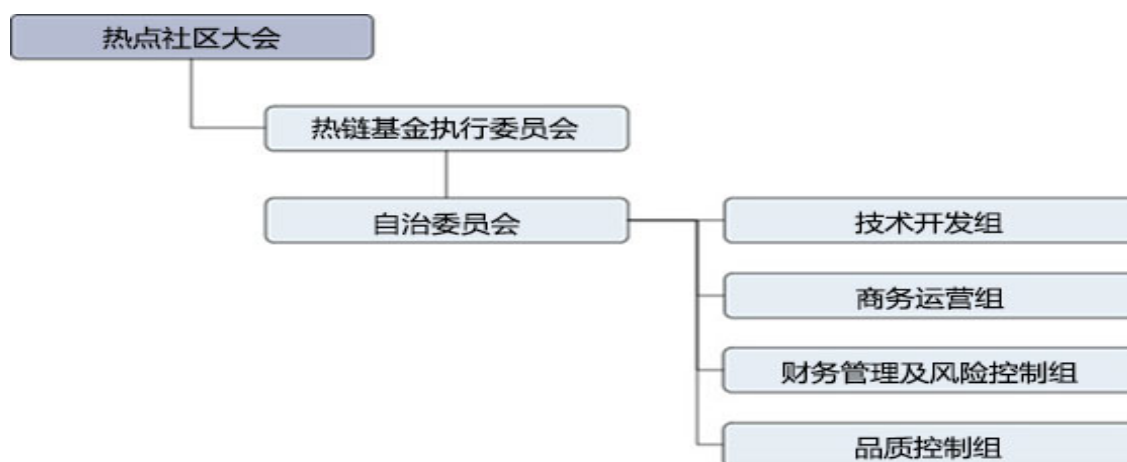


图 7 热链基金会组织架构图

首届热链基金自治委员会在项目中扮演着关键角色，首届自治委员会成员由热链核心团队担任。自治委员会任期届满后由社区根据热点持有数量和币龄计算权重，产生 100 名社区代表，再投票选举，最终产生 10 位自治委员会成员，代表热链基金会完成决策，并在任职期间接受信任调查。只有超过三分之二的自治委员会成员表决通过的决议，才可被采纳执行。

5.1.1 热链社区大会

热链社区大会由全体热点持有人组成，是热链（HeatChain）的最高权力机构。具有如下职能：

- 修改热链管理条例；
- 监督热链管理条例的实施；
- 选举和变更自治委员会委员；
- 撤销自治委员会的不当的决定；
- 批准重大变更事项；

社区大会所做出的决议，需经持有人根据热点数量和币龄计算权重进行投票表决通过。热链管理条例是热链自治的根本准则，管理条例将在热链官网公示。热链上线试运营半年内公布热链管理条例。第一版管理条例由自治委员会制定公布。社区大会每二年召开一次，若自治委员会认为有必要，或者五分之一以上热点持有人提议，可临时召开社区大会。

5.1.2 节点管理委员会

热链的使命之一是为量子产业相关应用提供底层基础设施，这里面涉及到对科研机构上传的技术成果做有效和真实性确认，同时对在热链上发起众筹的量子产业项目做可靠度和尽职调查等业务工作，因为涉及到技术专业性和法律合规性及金融的风险性，所有的工作都是由授权的超级节点来完成；所有热链在面向所有人开放的同时，也会对链上节点的加入进行一定的管理，这种管理机制不是中心化的体现，而是一种为帮助热链达成自身使命所必须搭建的自理机制。热链的第一批节点将包括国家顶级量子科研部门及实验室、互联网公司、高校、云服务提供商、量子技术资产交易中心、上下游产业链中的相关参与者等，这些节点的参与将赋予热链极高的可信任性和专业性。所有加入热链的节点将共同组建成为节点管理委员会，对后续申请加入

热链的新节点进行管理。我们将制定记账节点准入标准，这一标准将综合行业背景、专业性、团队成员、应用场景、技术和硬件能力等因素，任何满足准入标准的第三方或用户都可以申请成为记账节点，由节点管理委员会完成节点加入的审核，决定其是否能够成为热链节点，参与记账。

5.2 风险管控

交易安全：

热链（HeatChain）通过区块链共识、不可篡改等技术以及数字签名、终端用户加密钱包等安全手段确保用户账户及资金安全；量子技术资产交易中心将提供金融级的安全服务；数据存储、网络等资源高效整合，将数据、应用、交易集成到区块链云中，构建安全交易网络环境。同时，还有其他一系列手段，确保热链安全和值得信赖。

5.3 财务管理与审计：

热链基金委员会必须保持高标准的诚信和道德的商业行为标准；遵守相关的法律法规及行业自律原则；热链 HeatChain 每年会邀请国际知名第三方审计机构对热链基金会的资金使用、成本支出、利润分配等进行审计和评估；热链 HeatChain 将无保留的公开第三方机构的评估和审核结果。

6 热链团队及顾问

6.1 团队介绍

成员	简介
黄发隆 发起人	热链（heatchain）创始人、区块链早期参与和实践者 2014 年风靡全国的派卡模式联合创始人 广东派卡网络科技 CEO
郭巍 联合发起人	中国生产力促进中心协会副主任 北京华国昆仑科技有限公司董事长
郭海峰 联合发起人	热链联合发起人 区块链底层及业务平台总架构师，南京时迈邦创始人 /CEO，亚欧国际科技评价中心 IT 委员会秘书长；吉林大学计算机软件学士；荷兰马斯特里赫特管理学院 MSM 硕士。长期从事国际技术合作、加密通信软件、移动互联网、云计算、区块链系统规划设计和研发工作。
赖晖 系统架构师	资深全栈工程师，江苏科技大学计算机学士，长期从事大数据与区块链技术的研究。熟悉 Hadoop 平台的部署、运维和相关故障解决，熟悉 HyperLedger、HDFS、Hbase、Spark、Kafka、Hive、IPFS 等组件的工作原理和应用开发。

<p>印海华 核心区块链工程师</p>	<p>南京师范大学学士；多年从事软件项目的研发和管理，曾任法国电信-皓都联合创新中心技术主管。组织了多个通信、安全项目的研发和实施。特别是对桌面/移动客户端前、后端项目实施具有很强的经验和能力，精通区块链技术、钱包产品的研发和系统管理。</p>
<p>余晓轩 核心区块链工程师</p>	<p>曾在多个公司担任核心研发。有 8 年的软件设计、研发的经验。对区块链、物联网、ERP 等行业有较深入的理解。</p>
<p>王海拉（法国） 系统规划及国际技术合作顾问</p>	<p>现任法国电信集团移动通信/云计算/信息安全领域的全球创新及商业拓展主管，巴黎第十一大学、北京邮电大学博士生导师。本硕毕业于法国最著名的巴黎综合理工学院(Ecole Polytechnique), 法国巴黎大学，博士；美国加州理工学院，博士后。 1988-2000，世界 500 强企业法国电信集团，历任部门主管，总监，VP 等职位；2001-2003，全球最大的跨国电讯服务公司 Equant 全球副总裁，负责 VoIP 和 PKI 等业务的运维和技术支撑；2004-2012，任法国电信集团北京法国电信研究院 CTO 兼 CEO，法国电信集团中国区首席代表。</p>
<p>Martin Vorbach （德国） 高性能计算顾问</p>	<p>欧洲航天局人工智能芯片专家，美国 Hyperion-Core 公司 CTO。做为顶尖高性能微处理器架构设计师，可重构计算领域屈指可数的顶级专家，毕业于德国著名的 KIT（卡尔斯鲁厄大学）。自 1986 年起，从事 Transputer（做为当时全球第一种并行架构的计算机）的开发工作。在 1996 年，合伙创立 PACT XPP,担任 CTO，并成功的将其产品推广到全欧洲和北美。Martin 目前是 120 余项 FPGA，DSP，superscalar 和异构架构处理器的全球、北美，欧洲专利的第一和最主要发明人。全球知名半导体厂商如 Xilinx，Altera，Lattice，以及 Intel 等目前也一直在使用 Martin 的很多专利。</p>
<p>Christophe Bavière（法国） 国际投融资合作顾问</p>	<p>泛欧洲私募股权基金 IDINVEST PARTNERS 及 CHANCE 投资平台 CEO 及管理合伙人。 CHANCE 的命名是由 CHina（中国）和 FrANCE（法国）两字缩合而成，2015 年 7 月 2 日，中法两国总理共同见证了其成立。Chance 目标是填补中欧面临的融资和技术缺口，专注于健康、环境科技、金融科技、数字科技和食品加工领域的法国及欧洲中小企业。</p>

6.2 专家顾问

成员	简介
姚昆仑	毕业于中国科学技术大学，获理学硕士、理学博士，中国科普作家协会会员，原国家科学技术奖励工作办公室处长。 贯彻执行科学技术奖励政策和法规，社会力量设奖登记与管理，科技成果登记、评价、鉴定等的组织管理工作。
王宇	原国家科技部政策法规司副司长
李士杰	北京大学产业技术研究院副院长、 北京大学科技开发部副部长兼北京大学技术转移中心主任
袁峰	沈阳工业大学管理学院副教授， 硕士研究生导师、主要从事电子商务和网络营销研究。
Seeram Ramakrishna(席睿释) 国际科研成果产业化顾问(新加坡)	新加坡国立大学副校长，纳米纤维和纳米技术中心的主任，英国皇家工程院外籍院士，新加坡工程院院士，印度国家工程院院士，东盟工程技术院院士。剑桥大学材料科学工程专业的博士学位；积极推动聚合物纳米纤维在材料科学、制备技术和设计方面的发展，在多个科学领域进行了独创性的研究，在纳米科技领域做出了巨大的贡献。在成果产业化方面，他参与成立了几家新加坡公司，例如 Electrospunra、ElectrospinTech、BioMers 等。
黄平	中国国际技术转移中心 北京技术交易促进中心主任 目前主要负责中国国际技术转移中心、国家技术转移集聚区、首都创新大联盟、首都科技条件平台等科技创新创业服务工作的建设和推动。在打造国际化技术转移枢纽、促进区域合作与对口支援等方面开展了大量工作，成绩显著。

7 热链 HEATCHAIN 发展历程及项目时间规划

时 间 规 划

2015 年 5 月 热链早期派卡团队开始进入区块链技术应用领域

2016 年 3 月 热链早期团队完成区块链+量子技术应用的核心使命与功能布局，并开始架构设计与构建工作，

2016 年 7 月 热链正式团队组立，横跨区块链底层技术、量子信息技术研究、管理、运维各领域尖端人才

2018 年 4 月 热链经济白皮书正式发布

2018 年 5 月 热链基金委员会在新加坡成立

2018 年 10 月 热链量子技术数字资产交易中心测试版上线

2018 年 12 月 热链正式版正式上线

热链基金会持续拓展与权威的量子技术的科研机构开展合作，目前拟作为热链的早期参与者的合作伙伴有：

◆中国科学院量子信息重点实验室郭光灿院士领衔的科研团队

◆中国科技大学潘建伟院士领衔的合肥微尺度物质科学国家实验室

◆中国科学院院士姚期智领衔的清华大学交叉信息研究院技术团队

◆优秀的德国与法国软件开发团队，将与热链团队一起持续系统升级；同时，热链基金会正在与几个高校建立联合实验室，从而有针对性地解决问题，形成联合创新孵化器，为优秀的量子技术创新提供有效的资金、资源及技术支持。

4.后续持续更新迭代和高校合作方面：

热链基金会积极开拓与世界高校之间的多种形式的合作，目前拟推广合作高校有：

●中国：清华、北大、中科大、浙大、哈理工、电科大等

●美国：哥伦比亚、斯坦福、麻省理工等

●欧洲：剑桥、牛津、法国等

大众科普：热链基金会正积极在全球各地开展多种量子技术科普活动，教育科普活动等

8 总结&展望

目前国际间的量子科研与商业备战已经进入白热化，因为量子技术商用化的成本投入巨大，目前还没有普及到民用市场和惠及广大民众，存在市场过小又在没有明显预期的情况下难有资本持续投入的情况下；迫切需要解决量子技术商用项目建设，全民主动参与的自发性问题。热链的任务就是希望建立社会经济学模型，探索出一个量子技术应用领域的强大的协作多赢模式，从而可以支撑全球可持续协作的量子商业化计划。

区块链技术的出现不但是一种技术应用的大革新，更是一种人与人合作的生产关系的变革。它让信任变的易得，让合作变得简单，为大规模的人之间的协作提供了良好的基础。热链基金会致力于通过区块链的思想来探索这样一种共识机制，去解决人们如何利用量子信息技术来创造更加美好的生活方式和愈发灿烂的人类文明。热链基金会希望建立的社会经济学模型，就是要利用热链的通证系统建立量子信息产业领域的生态链，让每一位参与者和贡献者都获得公平的回报，通过这种社会经济模型吸引更多的资源体参与量子技术领域的产学研建设，并无限拓展人类的认知边界。

放眼更长久的未来，随着热链的持续成长与开放，应用、内容和数据的积累，当这些与热链的分布式经济模式相结合，将会是一件了不起的事情，它将第一次真正意义上，在实现在去中心化的条件下，打破国家安全和利益壁垒，从而将整个量子科技产业推向一个全新的模式和境界。