光子盒

2021量子技术全景展望

2021 Quantum Technology Insight

目录

第一章：前言

本报告由光子盒根据 Fact Based Insight 文章整理而成。

近年来，世界各国高度重视量子技术发展，通过出台政策文件、成立研究机构、支持量子科技研究等方式加大对量子研发的投资，促进量子科技研发和产业发展，试图在未来建立量子生态系统。

全世界的政府已经意识到，量子是一系列相关技术的未来机遇，不仅涉及量子计算领域，还在传感与测量、通信、模拟、高性能计算等领域拥有广阔的应用前景。并且，这些量子生态系统及其整个供应链之间存在联系。

各国政府已做出响应，启动量子技术计划，以发展这一重要的未来科学技术。2019 年，各国政府争先恐后地达成了一项 10 亿美元的计划用于量子计算研究。2020 年，对于该研究所需的支出和想要达到的成果都显著增加。

世界各地的专家已经撰写了许多有关量子领域的文章。本文重点关注 2020 年的关键发展，以及它们告诉我们在 2021 年要注意的事情。为了支持以下观点，Fact Based Insight 可以提供文章撰写的独立性，并没有从这些计划中获得任何资助。

第二章：主要国家的量子发展路线图

一、欧洲

欧洲很早就意识到量子信息处理和通信技术的潜力。除了 2016 年推出的“量子技术旗舰计划”外，还通过调整其他计划（例如其数字和太空计划）的支出，增加其可用资金，为实现未来的“量子互联网”远景奠定基础。2020 年 5 月，欧盟“欧洲量子技术旗舰计划”的官网发布了《战略研究议程（SRA）》报告。

10 年内，估计欧盟在整个量子技术旗舰计划中的相关量子支出为 30-40 亿欧元。

“量子技术旗舰计划” 全程开放式运作，不仅促进了每个项目各成员国内部的协作，还促进了项目之间的协作。该项目有 60 项专利申请（虽然欧洲在上述领域诞生了一些最优秀的研究，但全球其他地区申请的专利数量更多），还通过出色的欧洲量子周之类的活动展示了自己的形象，同时也使研究进展更加透明。

欧洲量子周计划是从一个以物理为主的兴趣小组动员起来的。该计划正在努力吸引更多的工程、计算机科学和数学人才。

“旗舰计划”——在拓展阶段，这个计划中的 19 个项目遍及量子计算、通信、模拟、传感和计量以及基础科学。2020 年，这些项目通过了中期审查，同时启动了两个新项目——QLSI

将硅自旋量子比特添加到已经成为目标的超导和离子阱量子比特的行列中；NEASQC 专门针对 NISQ 应用程序，解决许多人认为缺乏软件重点的程序的平衡问题。

EuroQCI 汇集了 25 个欧盟国家、欧盟委员会和欧洲航天局，其具体目标是建立泛欧量子通信基础设施，设想了将在 10 年内部署的两个关键要素：现有光纤设备间互联链路的地面站接收系统以及基于远距离双方之间的空间链路。第一个服务是 QKD，其他服务也会接踵而至，例如数字签名、身份验证以及超精密时间信号的同步。

Thierry Breton（欧盟专员，前 ATOS 首席执行官）强调另一个重要的目标是“促进欧洲世界级量子通信技术产业的发展，从而增强我们在这一关键领域的技术主权”。OpenQKD 对这一计划进行了补充，通过提供测试平台来演示各种客户端的使用案例。

HPC ——欧盟追求的百亿亿次（E 级）超级计算机是中国、美国、日本都在追求的高性能计算的前沿技术，目前都未完全实现，故研究量子计算的目标与委员会捍卫欧洲在 HPC 中的地位目标相吻合。

Breton 确表示：“我们的目标是使用百亿亿次计算机快速达到计算的下一个标准，而且最重要的是已经集成了量子加速器以开发混合动力机器，这种颠覆性技术将会使欧洲处于领先地位。”

欧盟的关键政策目标是确保欧洲成功进行数字化过渡。地平线 2020（2014-2020）对欧盟的研究与创新计划提供了支持，该计划后续将由欧洲地平线（2021-2027）接替，这就是量子技术旗舰计划资金的主要来源，也是数字化议程中的优先事项。

该程序目前正面临不利因素。英国脱欧，COVID-19 危机以及一些中欧国家向民权的转移，为欧盟的预算程序掀起了一场风暴。委员会对大幅增加欧盟“地平线 2020”计划中预算的提案有所异议。尽管这并没有威胁到该计划的现状，但它限制了计划中增加预算资金的范围。为了改变这种情况，委员会开始从各方寻求资金。

传统上，欧洲研究计划倡导开放科学，开放创新和对世界开放的价值观。准成员资格允许非欧盟国家参加其研讨活动，QuantERA 资助机制更鼓励各国在整个欧洲研究领域进行合作。因此，量子技术旗舰计划开始探索与加拿大，日本和美国的潜在合作。但是，确保数字或技术主权已成为欧盟目标中越来越重要的一部分，这包括限制中美两国利益的依赖性和影响力，这样的限制为未来计划开展中的包容性和灵活性带来了不确定性。

与其他量子计划一样，人力资源是重点领域。但是，仍有一个关键问题没有明确的答案——是说服有才能的欧洲学生不要去 Alphabet 和阿里巴巴工作，还是说服这种国际科技专业的学生更多地利用他们的价值在欧洲开展研究工作？

业务参与——欧洲许多大型企业都积极参与量子旗舰计划，特别是 ATOS、泰雷兹集团、空中客车、大众、博世和法国电力集团。然而，许多公司仍在寻求欧洲商业态度的更大的转变。量子技术旗舰计划主席 Jurgen Mlynek 表示：“美国科技公司更愿意进行长期投资。欧洲大公司说‘很高兴听到您在做什么，但我们是技术接受者，而不是技术制造商。’”

QuIC——正在准备启动欧洲量子科技产业化联盟。这被认为是美国 QED-C 的对应版本，目标是 200-225 个成员。

还有一个问题，使欧盟范围内的量子研究计划难以实施。许多人认为，未来量子生态系统中的社区将锚定在特定地理位置附近，硅谷在美国的成功就是一个典型的例子。与其在欧盟范围内直接建立这样的中心，不如借鉴各国在量子领域的成功案例更为现实。

许多欧洲国家都有重要的量子活动，包括奥地利，西班牙，匈牙利，波兰，瑞典等。其中，有 3 个欧盟国家和 1 个前欧盟国家脱颖而出，需要对这些国家做进一步的研究。

1. 德国

德国政府已经宣布，为应对新冠肺炎疫情冲击，将提供 20 亿欧元用于量子科技研究，为 2018-2022 年间计划用于量子研究的预算支出打下了基础。在 2020 年下半年，担任欧盟轮值主席国的德国再次强调量子技术在数据主权等方面的重要作用，同时，德国已经对非欧盟国家的相关高科技公司进行了更严格的限制。

德国已经拥有强大的量子研究基础，例如马克斯·普朗克研究所、亥姆霍兹协会以及弗劳恩霍夫协会，这些领先的研究组织已经独立参与了多个国家的量子技术项目。

Forschungszentrum Jülich 研究所在欧洲量子领域中地位逐渐上升。它是跨物理、化学、生物学、医学和工程学的大型多学科研究中心和大型超级计算机中心，并且已经启动了 JUNIQ 程序，以提供访问多种量子计算技术的平台。它将在 2021 年成为 EU QuIC 的研究总部，并托管 OpenSuperQ 交付的量子计算机原型。此外，它还将接手于 2025 年之前全面投入运营的亥姆霍兹量子中心。

MCQST 正在着手建造慕尼黑的量子谷，它已经获得了巴伐利亚州的 1.2 亿欧元支持。PlanQK 中包含德国工业界的著名先驱，如大众汽车和博世，也通过不断的发展成为虚拟量子集群软件。

2. 荷兰

荷兰已经成为量子研究活动的重要中心。于 2014 年成立的 QuTech 已经具有“国家标志”的地位。它与微软和英特尔等专业公司、BlueFors 等主要专家以及 Orange Quantum Systems、Qblox、Single Quantum 和 Delft Circuits 等有趣的初创公司建立了牢固的行业关系。

Quantum Delta NL（Q∆NL）计划利用荷兰现有量子技术资源进行协调合作：包括代尔夫特的 QuTech，阿姆斯特丹的 QuSoft 和埃因霍温的 QT/e 等研究机构；莱顿、奈梅亨、格罗宁根、特温特和乌得勒支的优秀研究小组，诸如 TNO 和 StartupDelta，以及一系列行业合作和初创公司。计划将集中在三个前沿领域，围绕五个城市枢纽——开展量子计算和量子模拟、国家量子网络和量子传感应用。

荷兰坚定不移地将本国定位为“通往欧洲的量子门户”，并期望建立量子硅谷，强调其中心的地理位置：高度的商业便利性和高质量的生活。目前，荷兰与微软和英特尔之间的合作关

系稳定,同时不断从QIA和iqClock等量子技术旗舰计划项目中受益。2020年,Quantum Inspire成为荷兰量子计算生态系统的一个重要里程碑，这是欧洲第一个基于量子云的平台。

3. 法国

法国已从量子领域集群以及相关的高科技产业专业知识中受益,与法国有着紧密联系的大型企业已经在量子领域取得了显著成绩，例如ATOS、泰雷兹集团和空中客车公司。

巴黎拥有量子计算中心以及著名的初创公司Alice & Bob、C12、Veriqloud、Qubit Pharmaceuticals和QC Ware France。

巴黎萨克莱（Paris-Saclay）成立了量子科学与技术跨学科中心。

格勒诺布尔拥有量子工程部和量子硅研发基地，并且还可利用CEA-Leti和CNRS-NEEL的优势。 CMOS工艺和低温CMOS电子学方面的专业知识使其成功开发硅自旋技术。

2020年初，法国推出了一项为量子技术构建一个国家战略的计划。由于发生了COVID-19危机，该计划暂时被推迟。此战略计划为科研和工业部署尖端量子计算基础设施投资。

4. 英国

英国的NQTP被认为是世界上第一个以开拓最广泛的领域为目标的量子技术计划，该计划横跨量子计算、通信、计时、传感和成像等领域。如今，该计划已被世界各地的专注于量子研究的国家所模仿。

2014-2024年，NQTP第1和第2阶段（包括公共和私人资源）的计划支出约为10亿英镑。

许多人将目光投向英国量子计划，不仅是为了评估英国的量子技术的进步，还会对自身知识的提升有所帮助。

NQTP第1阶段（2014-2019）已与英国自然科学基金、英国基础设施建设局、英国科学与技术设施理事会、英国国防部、英国国家物理实验室、英国商务能源与产业战略部以及英国政府通信总部合作。最初建立了四个量子技术中心，重点研究量子计算、量子通信、量子增强成像和量子计时与传感。
结果——在初始阶段提供了一系列出色的原理证明。它还发动社区活动并形成了学术、产业合作的模式。项目最初是建立在英国光子学上，是跨所有量子基础的一项关键技术。该计划的成功为工程师工作带来了灵感。受益于数学和计算机科学人才的引进，英国量子软件领域愈加充满活力。

NQTP第二阶段（2019-2024）将重点和资源转移到商业主导项目上。随着产品越来越符合市场要求，合作伙伴通常希望对将要成型的计划采取更多控制，以确保能从该计划提供的协作框架中受益。作为回报，Innovate UK利用产业战略挑战基金(ISCF)发起一系列由公共、私人混合资金支持的项目，以支持不断发展的量子生态系统的搭建。

进行中—— Innovate UK 团队非常重视计划管理和加强计划倡议的商业展示。

现在，重点研究已经转移到了量子价值链上。对单个量子和叠加的关注已经转移到了量子纠缠的可能性上。

成像——英国计划将量子增强成像作为自己的研究支柱。英国的计划瞄准了细分市场中的机会，还刺激了潜在的量子光子生态系统，并开发了重要的传感技术。

NQCC 是第二阶段的另一个主要目标。NQCC 不是设想成为量子计算竞赛中的一个直接竞争对手，而是作为一个工具，加快社会效率。

升级——物理中心的设计现已完成，后续建设工作将持续到 2021-2022 年，计划于 2023 年第一季度交付使用。最初，该中心将超导、离子阱和软件作为优先研究领域，但该中心的资金是用于对量子领域的投资，而不是特定的量子技术。

ISCF（产业战略挑战基金）目前正在资助三个重要量子研究领域中启动的 40 多个量子项目。通常，每个财团都会聚集来自整个供应链的 3-10 个合作伙伴，并提供强大的学术支持。项目通常设置为运行 18-36 个月，预算在 50-1000 万英镑之间。这种方法具有一定的灵活性，可以在后续开发补充项目，同时可以支持多种项目类型。

可行性研究——通常针对较小的项目，例如 Gravity Delve 计划，旨在探索在恶劣的中心环境中使用量子重力传感器的能力，该计划与另一个重力传感器计划 ABGRAV 同时进行。

协作研发——大型项目将供应链参与者聚集在一起，以更高效对产品进行升级。研发重点通常是确保有可行的供应链来支持产品的商业化研发模式，并且可以从可能的参与者手中获得投入。例如 KAIROS，这是由 Teledyne e2v 领导的将紧凑型原子钟商业化的计划，或由 Rigetti 领导的在英国建造量子计算机的计划。

技术项目——大型项目，以建立更广泛的生态系统，该项目用来部署新的基础结构。例如，由牛津量子电路（OQC）牵头的用于制造和测量的 Quantum Foundry 计划，以及由 Riverland 牵头的提供与硬件无关的软件堆栈的 Deltaflow.OS 计划。

人才教育是英国量子计划的另一个重点。

QTEC 是英国 NQPT 第一阶段的一项计划，为科学家转变为企业家的过程中提供帮助。“奖金”将为早期从事相关工作的研究人员提供薪水、费用、业务培训和指导，为他们提供为期一年的创业指导。现在，QTEC 的早期研究员正在参与诸如 KETS 和 Seeqc 之类的量子领域后起之秀的培训工作，或者在特定领域的（例如 QLM 或 FluoretiQ）商业化应用方面取得了令人瞩目的进展。Nu Quantum 和 Quantum Dice 是最近两个知名的初创公司。

Fact Based Insight 认为，QTEC 已经取得了显著的成功。但是目前，NQTP 的第二阶段尚未为其继续提供资金。它最初的出资者是英国自然科学基金(EPSRC)，但是，EPSRC 的核心目标正集中在科学研究和培训上。同时，Innovate UK 一直在努力发起 ISCF 项目。Fact Based Insight 希望，NQTP 能继续开展其计划的第二阶段。

NQTP 希望使英国成为量子企业和量子人才的“理想之地”。此前 PsiQ 公司由于在欧洲很难申请到科研基金，故将公司搬到了硅谷。

在 NQTP 的第二阶段，英国量子计划取得了显著成就。Rigetti 和 ColdQuanta 等美国公司也开始被英国的量子研究环境所吸引。Teledyne e2v 和 Hitachi 已将其在英国的子公司用于扩大其在该领域研发的基地。东芝正在英国制造 QKD 设备。充满活力的量子研究环境已经初步形成。

“欧洲地平线”计划——英国是否继续参与欧盟的主要研究计划是整个社会的主要不确定因素。从欧洲研究计划获得的资金份额而言，英国在量子领域的研究做得很好。更重要的是，它已经很好地受益于当前建立的研究关系网络。

英国的 NQTP 计划早于欧洲量子技术旗舰计划，但是，随着旗舰计划的实施，欧洲大陆所扮演的核心角色作用日益凸显，并且从量子技术旗舰项目上的交叉合作模式的成功案例中说明这是双赢的局面。

英国政府一直宣布要参加“欧洲地平线”计划，欧盟领导者也在推进英国与该计划的合作。不幸的是，欧盟和英国之间就脱欧协议达成的贸易谈判使英国参与该计划产生不确定性。

英国继续在全球各地建立牢固的研究合作关系。2020 年英国量子技术展示会的主题演讲是宣布加拿大、英国联合融资。尽管融资数额不大，但是作为旨在支持量子技术商业化的计划的一部分，这是值得注意的。

Fact Based Insight 认为，英国正不断为量子融资寻找渠道。

在首相鲍里斯·约翰逊的政策中值得注意的一点是计划大幅增加公共研发支出，并建立一个新的机构，用来进行高风险、高回报的研究，即英国的 ARPA 计划。但是，鉴于它与英国研究与创新机构(UKRI)的关系，关于如何实施这一计划仍在考虑中。UKRI 本身是一个相对创新的部门，它汇集了包括 EPSRC 和 Innovate UK 在内的英国主要研究资助组织，这两个组织是英国 NQTP 的主要资助来源。

包括 Dominic Cummings（现任首相顾问）在内的英国 ARPA 核心支持者都希望将其视为一个新的独立机构。乔·约翰逊（前科学部长、首相的弟弟）和马克·沃尔波特（英国 NQTP 联合创始人）都认为 UKRI 是“孵化 ARPA”的理想基地。UKRI 的核心研究预算将在未来三年中以每年 4 亿英镑的额度增加。另外，高风险、高回报基金的首笔 5000 万英镑资金在 2021-2022 年用于 UKRI，基金中的 8 亿英镑将在 2024-2025 年拨款。这些资金大多会用于量子领域的研究中。

二、北美

1. 加拿大

加拿大在现代量子科学方面有着杰出的贡献。尤其是在 1984 年 Gilles Brassard（蒙特利尔大学）提出了著名的 BB84 量子密码协议。2002 年，加拿大首创的量子计算研究所（IQC）在滑铁卢大学成立。在 2008-2018 年，量子科学和技术投资超过 10 亿加元。

2017 年，加拿大国家研究委员会(NRC) 发起了一个名为 Quantum Canada 的计划。对于加拿大来说，总部位于加拿大或与加拿大有紧密联系的知名量子公司的数量众多。例如 D-Wave、Xanadu、1QBit、Quantum Benchmark、evolutionQ、Zapata 和 ISARA。其中，创意破坏实验室(CDL)一直是量子行业初创企业的标杆。

到 2020 年，加拿大量子产业通过成立新的产业联盟，来巩固这一地位。2020 年，温哥华的数字技术超级集群也宣布共同投资资金达 1.53 亿加元。

2. 美国

美国在量子科学方面的投资历史悠久。2020 年是美国国家量子倡议(NQI) 计划的第二年，并且随着该计划的真正成形，人们也看到了量子科技发展的亮点。NQI 将在 2019-2023 年支出 13 亿美元，大量私人资金也已投入其中。

在美国国家科学基金会设立了三个新的量子飞跃研究所。这些以学术为主导的研究所将支持不同领域的研究。

Q-SEnSE——纠缠科学与工程的量子系统（由科罗拉大学博尔德分校领导）。采用量子传感技术在精密测量中广泛应用。

HQAN——混合量子架构和网络（由伊利诺伊大学香槟分校牵头）将开发用于离子阱、中性原子和超导量子比特系统的多节点试验台，以及分布式量子计算软件堆栈。还致力于下一代容错量子比特，同时与芝加哥量子交易所合作密切。

PFQC——当前和未来的量子计算（由加州大学伯克利分校领导）。设计大规模量子计算机，为当前和未来的量子计算平台开发有效算法，并验证量子计算机能超越经典计算机。

美国能源部拥有一个由 17 个国家实验室组成的独特网络，在美国研究领域具有独特的能力。美国能源部已经建立了五个国家量子信息科学(QIS)研究中心。

Q-NEXT——下一代量子科学与工程（阿贡国家实验室）。将专注于长距离量子网络，量子使能的传感以及处理和测试。它将建立两个用于材料和器件制造的国家量子铸造厂。著名的合作伙伴包括英特尔、IBM、微软和 ColdQuanta。

C2QA——量子优势协同设计中心（布鲁克海文国家实验室）。旨在克服早期 NISQ 设备的局限性，以实现高能、核、化学和凝聚态物理科学应用中的量子优势。五年目标是在软件优化，基础材料和设备特性以及量子误差校正等各个方面改进 10 倍。著名的合作伙伴包括 IBM。

SQMS——超导量子材料和系统中心（费米国家加速器实验室）。通过了解引起退相干的物理过程，专注于创建更好的超导量子比特。旨在利用下一代超导量子比特技术构建量子计算机。

著名的合作伙伴包括 Rigetti。

QSA——量子系统加速器（劳伦斯·伯克利国家实验室）。旨在共同设计在科学应用中提供认证的量子优势所需的算法、设备和工程解决方案。重点技术包括中性原子、离子阱和超导量子比特。桑迪亚国家实验室是主要合作伙伴。

QSC——量子科学中心（橡树岭国家实验室）。发现、设计和演示拓扑量子材料，利用拓扑系统的算法以及用于测量异常微弱信号的新量子系统。微软是五个核心成员之一。其他合作伙伴包括 IBM 和 ColdQuanta。

同时，每个研究机构还强调它们在培训和劳动力发展中扮演的角色。此外，国家 Q-12 教育合作计划旨在改进所有教育中心的量子学习课程。

国家标准与技术研究院(NIST)是美国计划的另一个关键部分。NIST 处在许多高性能量子技术（特别是在离子阱和量子时钟中）研究的最前沿，其中的一项关键活动一直在支持 QED-C 的创建。

QED-C 作为利益相关者的联盟，其使命是促进和发展量子产业及相关的供应链。由 SRI International 管理的财团得到政府以及来自各行业、大学和国家实验室的 160 多成员的支持。

QED-C 汇集了来自量子生态系统各个方面的专家，以识别并帮助填补技术、行业标准以及员工队伍方面的空缺。

QED-C 将继续找出技术差距，并与政府和行业合作伙伴合作填补这些差距。Celia Merzbacher（QED-C 副主任）强调“ QED-C 成员期望将全球网络作为量子供应链，我们将在 2021 年提供非美国会员制合作机制”。同时也希望 QED-C 将重点放在建立多样化的人才培养上(包括来自少数族裔服务机构的人才）。

白宫的国家量子协调办公室（NQCO）和国家量子计划咨询委员会（NQIAC）是美国量子协作业研究的总协调机构，以促使来自大型技术，国家实验室和量子领域领先科学家的共同协作。

AFRL ——备受推崇的空军研究实验室一直是美国量子领域的先驱。它拥有跨时序、传感、通信和计算（算法）的大型联合程序。

DARPA ——该研究机构及其前身 ARPA 使它在量子领域具有一定的地位。过去的研究成果对量子技术的早期发展产生了影响，特别是用于原子钟的 CSAC（2001-9），用于量子感测的 QuASAR（2010-18），用于量子计算和通信（包括世界上第一个 QKD 网络的演示）的 QuIST（2001-5）。当前值得注意的成果包括用于创建 NISQ 量子计算机的 ONISQ 和用于开发具有独特拓扑特性材料的 TEE，这些材料可用作拓扑量子比特以及其他潜在应用。著名的研究合作伙伴包括 Rigetti 和 ColdQuanta。

IARPA ——受 ARPA 的启发，该机构制定了许多有影响力的量子计划，包括 CSQ（2009-14）

超导量子比特技术；MQCO（2010-15）扩展挑战；关键算法的 QCS（2010-13）资源基准。目前的计划包括有关逻辑量子比特开发的 LogiQ（2015+）等。

该计划早期战略方向是强调量子网络的价值。在美国能源部启动量子战略之后，美国国防部根据美国能源部的 17 个国家实验室的初始骨干网络，提出了量子互联网的战略蓝图。

为了实现这些目标，2020 年向国会提交了两项相关法案，但这些法案没有获得通过。

《量子网络基础设施法案》（Quantum Network Infrastructure Act）：加速为美国量子网络提供基础的研发，五年内计划投入 5 亿美元。《量子科学和技术用户扩展法案》（QUEST）：支持对量子计算资源的研究访问，五年内计划投入 3.4 亿美元。

美国已对量子领域的研究做出了下一步计划。新一代超导量子比特技术是一个重点研究领域，紧随其后的是离子阱和中性原子平台的研究。对于算法、软件平台和量子感测也应给予关注。

许多新研究中心也强调了对学科应用的重视。过去的经验告诉我们，科学应用程序所开创的先进技术随后会应用到更广泛的领域。但是，这确实代表了工业合作伙伴（正如在英国计划的第一阶段中看到的）的潜在威胁，在某些情况下，这些合作伙伴在项目重点方面会与学术研究者有所不同。

NQI 程序已完全启动并运行。鉴于它坚实的基础，我们可以期望在未来的几年中，会取得令人振奋的成果。现在的疑问在于，美国计划的实现将在多大程度上依赖与国际伙伴的合作。

三、中国

中国“五年规划”（尤其是自 2006 年以来，包括量子科学）一直推动着科学和技术领域的发展。中央和省级资金已经投入超 15 亿美元，中国科学技术大学已经成为世界上主要的量子研究中心。迄今为止，中国拥有全球最大的已部署 QKD 网络，并在先进空间量子通信技术方面继续保持世界领先地位。“墨子号”卫星和九章量子处理器是该计划成功的标志。

2006-2020 年，中国计划支出的 10 亿美元来自中央，5 亿美元来自地方。据官方媒体报道，到 2022 年，该投资将达到近 150 亿美元（1000 亿元人民币）。

正在建立量子信息科学国家实验室（NLQIS）的网络。

NLQIS 合肥：将成为世界上最大的量子研究机构以及该计划的总部。将重点关注光子、金刚石 NV 色心和硅自旋量子比特技术以及量子通信和量子感测。

NLQIS 北京：该分支将专注于理论、离子阱和拓扑量子比特。

NLQIS 上海：该分支将专注于超导量子比特和超冷原子以及自由空间量子通信。

中国的国家量子网络将继续发展，以使其更安全，更快速，更广泛。

纵向骨干网：最初的 2000 公里京沪线正在扩展，目前正在建设 5500 公里的延长线。

横向骨干网：合肥和武汉之间已经完成了 700 公里的横向骨干网建设，另外 360 公里正在建设中，拟建 2200 公里。

卫星：用于开发启用 QKD 的纳米微卫星群的高级程序。

阿里巴巴、百度、腾讯和华为都在量子技术上进行了量子投资。国盾量子和本源量子是著名的创业公司。

“十四五规划”详细介绍了该计划，计划将于 2021 年正式通过。一个关键概念是“双循环”，包括减少对外国高科技的依赖，同时增加对外国投资的开放度。同时，创新也是一个关键主题（提案草案中提到了 47 次）。

量子技术将成为高科技领域的重点之一。在草案发布前夕，习近平主席借此机会亲自强调了发展量子科学和技术的重要性和紧迫性。同时，中国 AI 和航空计划的持续发展也互为补充，也着重规划了量子科技到 2035 年的路线图。

《中国标准 2035》的目标之一是在确立领先技术的通用规范方面建立中国领导地位。

四、来自世界各地的量子科技发展

1. 澳大利亚

澳大利亚的量子研究部门非常活跃，特别是 EQUS 和 CQC2T，并形成了多元化的量子创业公司，其中包括新南威尔士大学(UNSW)衍生公司 SQC 和 Q-CTRL 以及 Quintessence Labs。

在主要的量子国家中，澳大利亚几乎没有单独的量子战略计划。然而，2020 年，澳大利亚联邦科学与工业研究组织(CSIRO)制定了发展澳大利亚量子技术产业的战略，并成立了澳大利亚量子技术论坛（AusQuantech）以促进该行业发展。

2. 日本

2018 年，日本政府于 2018 年推出 Q-LEAP (Quantum Leap)计划，其中日本科学技术振兴机构(JST)第 2 期战略性创新推进计划（SIP2）与量子传感、量子软件、量子密码有着紧密的联系。

2020 年初，日本量子技术和创新战略初步完成，优先研究领域包括量子模拟与计算、通信和传感。

日本在 2018 年启动了新的项目，包括超导量子比特 NISQ 计算机和 NISQ 软件程序。

“Moonshot”研发投资计划预计将投入约 150 亿至 200 亿日元，希望在 2050 年之前制造出容错通用量子计算机。

3. 俄罗斯

俄罗斯量子中心（RQC）成立于 2010 年。俄罗斯的量子研究得到了当地政府和工业实体的支持。到 2020 年，已形成三个单独的量子研究路线图，每个路线图都针对不同的量子领域基础。有趣的是，每个支柱都由一家俄罗斯大型国有公司领导：俄罗斯国家原子能公司负责量子计算和模拟；俄罗斯铁路局负责量子通信；俄罗斯国家技术集团负责量子传感和计量。

4. 新加坡

2007 年，新加坡政府帮助建立了 CQT（量子技术中心）。2020 年，它启动了一个新的为期 5 年的量子工程计划，其中，Quantum SG 的创建是该计划的重点。

五、全球学术合作

美国新政府将重塑美国的对外关系，但是大多数人认为中美关系将保持紧张。拜登仍可能将中国视为日益加剧的全球技术竞争对手。

由于担忧中国被赶超，导致 NQI 的支持开始动摇。在欧洲，欧盟的量子计划和德国的大规模量子新战略将以确保量子技术主权作为主要目标。中国重视“双循环”战略，强调技术自给自足。量子技术日趋商业化也日益吸引领先的研究人员从事该领域工作，最终将导致公开分享研究成果的机会落空。

尽管如此，我们仍在努力使全球科学话语的开放性。2020 年最受学术关注的会议是 IOP 和中国物理学会联合组织的 Quantum 2020。这体现了来自所有量子领域和所有主要量子研究国家的尖端贡献。

中国物理学会会长张杰呼吁量子的国际科学合作与交流。欧盟量子社区网络主席 Tommaso Calarco 在一个有关国际量子技术计划的小组发言中，呼吁采取一系列应对措施，以帮助量子社区保持其包容性。彼得·奈特爵士（英国 NQTP 的创始人）利用专家小组推进了世界范围内学术团体的“量子联盟”的构想，并在可能的情况下对基础科学问题保持开放性态度。这样的想法很可能会受到世界各地学者的广泛欢迎。

六、量子投资的时机

政府提供慷慨计划支持的原因之一是担心仅靠自身的力量，可能不足以看到量子革命。

一方面，2020 年是量子技术领域投资创纪录的一年，Interference Advisors 的报告显示 10.4 亿美元（至 11 月中），其中一半是来自 PsiQ 和 XTalPi 这两笔交易。另一方面，一些

知名的量子硬件厂商也已在 2020 年进行了缩减。从对比可看出，量子密码技术在西方吸引力不强，而中国国盾量子的 IPO 创下了首日涨幅纪录。

不确定性是存在的，但是，可以采取一些策略平衡这种不确定性带来的风险。量子硬件、软件、通信和传感通过许多常见的技术链接在一起。但无论是在宣传程度还是获取收益的时间线来讲，它们在商业上都不是同步的。迄今为止，我们认为 Quantonation 公司是量子信息时代的最佳投资组合策略者。

目前，许多大投资者都对保持自己的立场，而风险基金谨慎地选择了少数项目来支持。COVID-19 带来的破坏是非常真实的。目前，从许多公司或政府计划中获得资金支持对许多人来说是最简单的方法。

在 Q2B 大会上，John Preskill（加州理工学院）也评论了许多人对未来几年的担忧：“量子计算的寒冬可能出现，这也是一个严重的问题。”

同样，无论科学家是否有所突破，都会有无数人在填补量子理论的空白。在 2021 年，会有很多非常聪明的人努力做到这一点。量子投资者必须时刻做好准备。

七、2021 展望

中国的“十四五”规划——墨子号和九章的成功是建党 100 周年的一份巨大献礼。未来五年中国在量子、人工智能和天基技术领域的投资细节即将浮出水面。该规划将于 2021 年 3 月获得全国人大的正式批准。

欧洲的投资——越来越多的欧洲国家有自己的重要计划。未来 7-8 年，整个欧洲的投资能否超过 80-90 亿欧元?

地平线欧洲计划——地平线欧洲的国际参与将如何发展?（编者:我们现在知道英国会参加;加拿大或日本是否也会加入？）

量子技术旗舰计划——随着 2021-2027 年欧盟最终预算协议尘埃落定，期待下一波欧洲量子项目的投融资消息。

欧洲量子财团——QuIC 是量子技术旗舰计划中的一个核心财团；EQIC 是在欧洲光电子行业协会 EPIC 支持下成立的一个财团。这些财团能帮助他们的成员一起做什么？注意加拿大、澳大利亚和新加坡会有类似的财团。

欧洲核子研究组织（CERN）、国际热核聚变实验堆（ITER）计划或空中客车（AIRBUS）——欧洲已经推出了许多用于大规模科学、研究或商业合作的模式。请留意关于哪种模式最适合量子技术的重大创新的争论。

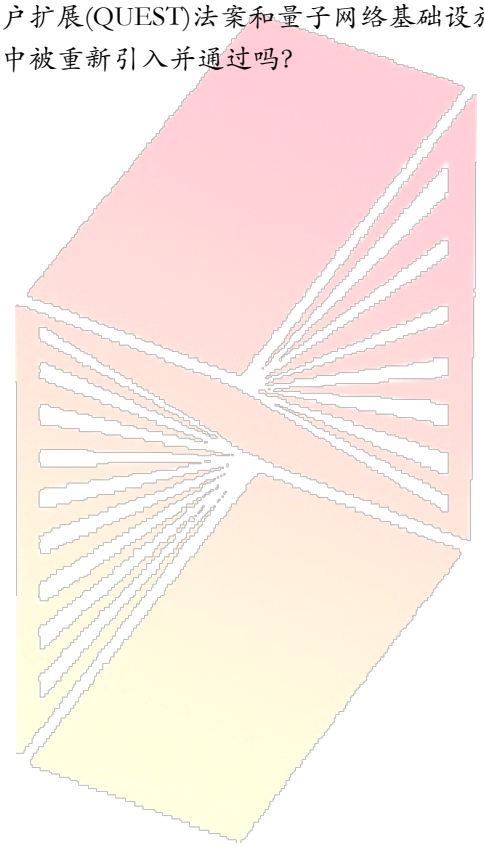
英国——注意通过产业战略挑战基金(ISCF)以及其他的高风险、高回报计划资助的更多量子项目。英国能否调动伙伴关系和资源来保持在量子方面的竞争地位?

日本——预计量子技术将在 2021 年初批准的日本第六个科学和技术基本计划（2021-26）中发挥重要作用。

俄罗斯——关注俄罗斯原子能公司(Rosatom)、俄罗斯铁路公司和俄罗斯国家技术集团(Rostec)主导的路线图的细节。

美国——有了三个新的国家科学基金会研究所和五个新的美国能源部研究中心，请注意这些美国发起的量子部门将掀起一场风暴。该计划能否证明它不仅仅是各部门的简单相加？

美国国会——关注量子用户扩展(QUEST)法案和量子网络基础设施法案的进展。NQI 的这些延伸法案会在新一届国会中被重新引入并通过吗？



第三章：2021 量子硬件展望

中国的量子优势论证登上了头条新闻，但尚未在量子计算竞赛中占据领导地位。领先的硬件团队已经为未来的马拉松确定了发展路线，而纠错已成为故事的关键部分。扩大规模的挑战仍然突出。

越来越多的量子专业公司、初创公司和研究机构开始打造范围越来越广的量子硬件。从早期的 NISQ（含有噪音的中型量子）设备到全规模的 FTQC（容错量子计算）设备。2020 年，中国的潘建伟团队再次吸引了新闻头条的关注，他宣布的量子优势论证声称将超过谷歌 Sycamore 在 2019 年实现的量子优势论证。就在那时，数学上关于计算到底有多难的争论也随之而来。

九章实验可能因完成了最复杂的计算而获得第一名，但在头条背后，这个新的里程碑有多重要呢？IBM 可以指出最大的云计算项目和高级用法的拐点。离子阱玩家（霍尼韦尔、IonQ）争相在量子体积上处于领先地位，但在量子比特数量上仍然落后。我们把这一切都放在一个背景下，看看在量子硬件领域发生了什么。

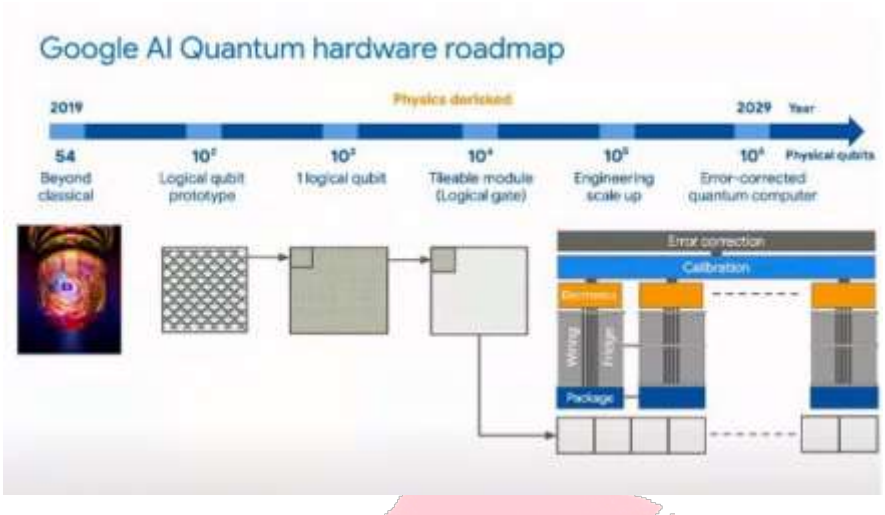
一、超导量子比特为重大突破做好了准备

1. 谷歌——过渡的一年

今年硬件行业的首个重大新闻是 John Martinis 离开谷歌，原因是与其领导层 Hartmut Neven 的关系紧张。在谷歌的量子夏季研讨会上，Neven 再次强调了谷歌计划的连续性，并概述了他们计划在 2029 年前建立一个拥有 100 万个物理超导量子比特的“小型”FTQC 的里程碑。

即使在离任时，Martinis 也一直在强调谷歌在程序和硬件方面的领先优势。然而，还是会有挑战。谷歌首选的可调谐量子比特和快速逻辑门提供了极大的灵活性和性能，但是 Sycamore 53Q 设备的校准显然是一个挑战。有了额外的控制，就需要在芯片上和芯片外路由额外的控制线。缩放比例会自动增加布线的挑战和元件数量与总体故障率之间的关系。值得注意的是，谷歌在 2020 年报告的大部分工作都使用了 Sycamore 的 23Q 配置，因为自动校准最初无法在较大的设置中提供可接受的 2Q 门性能。谷歌将材料研究作为提高量子比特相干时间的一种方法。尽管前景很好，但这需要科学的进步，而不仅仅是工程上的进步。

谷歌路线图——从现在到 2029 年：102Q（逻辑量子比特原型）、103Q（一个逻辑量子比特）、104Q（可平铺逻辑模块）、105Q（工程扩大）、106Q（纠错量子计算机）。通过表面代码协议进行错误纠正。



Neven 引用肯尼迪在阿波罗计划中的话：“我们可以在十年内做到这一点”。谷歌的近期目标是证明物理量子比特错误可以通过使用增大尺寸（码距）的原型逻辑量子比特系统地减少——有效地在实践中证明使用表面编码协议进行纠错，而不仅仅是理论中。

Neven 还特别强调创建约 10,000 个物理量子比特的可平铺模块。他认为这些是传统计算机设计核心的逻辑门的真正等价物。重要的是，它们代表了“物理风险在降低”，投资者仅需担心传统工程的挑战。谷歌的愿望是在 2025/2026 年左右达到这一目标。

2. IBM——蓝色巨人

IBM 很早就开始为其路线图打下基础。IBM 是推动教育更广泛的社区的先行者，重要的不仅是量子比特数量，还有量子比特连接、门集和可实现的电路深度（一个与门保真度紧密相关的指标）。基于这些属性，IBM 引入衡量量子计算机性能的指标——量子体积（QV）。

自 2017 年以来，IBM 已经交付了 28 款性能在稳步提高的系列设备。每年 QV 翻一番的既定目标，他们在过去一年中成功做到了两次。他们的 27Q 处理器达到了 QV 128 的水平，我们可以期待他们最近发布的 65Q 处理器会在适当的时候超越。到 2023 年，IBM 的目标是生产代号为 Condor 的 1121Q 处理器，将其容纳在一个新的稀释“超级冰箱”中。Goldeneye 冰箱目前处于原型阶段，旨在容纳多个芯片。

IBM 路线图 - ——2021 年 127Q（Eagle）、2022 年 433Q（Osprey）、2023 年 1121Q（Condor），从而形成 100 万量子比特的大规模系统。通过颜色代码协议进行纠错。

IBM 显然专注于大规模的 FTQC。Condor 最初的设计采用了与最近其他芯片相同的六边形的布局。这种低连通性设计是为了使具有固定频率量子比特设计的芯片更易于制造，同时旨在使用低连通性颜色代码而非表面代码来进行纠错。以确保他们的路线图在 2023 年时比其他公司更清晰。此外，IBM 的超级冰箱最终能够堆叠多个芯片，从而提供“数百万个”内部连接的量子比特。

在评估 IBM 能否实现目标时，很难不被它的过往记录所打动。IBM 还将大幅减少 2Q 门错误。尽管他们最近几代的处理器在该关键参数上均表现出稳定的改进，但是他们的计划现在似乎承认需要对他们的 2Q 门设计进行更重大的修改。

在保留固定频率量子比特以利用其允许的长相干时间的同时,IBM 一直在尝试在每个门使用额外的可调谐振耦合器和旁路电容耦合器。这保证了 2Q 门的速度更快(误差也更低)，但是由于相比与其先前技术设计发生重大变化，到目前为止，只有在简单的 2Q 实验设备中才能实现。

为了应对日益增长的布线挑战，IBM 开发了基于三层超导布线的下一代芯片布局。看到这些技术如何顺利地结合在一起，将是 IBM 路线图的关键测试。

在 IQT 欧洲峰会上，Lieven Vandersypen（QuTech 科学总监）指出，尽管很多人都希望更快地发展，但量子体积逐年翻倍仍然是一个挑战。我们需要回想一下，仅仅增加量子比特是做不到这一点的。同步操作中的 2Q 门保真度是目前的限制因素。Jay Gambetta（IBM）说：“我看到了未来的挑战，但没有障碍。”

3. 超导多样性

Rigetti Computing 下一代设备的概念是基于将多个 32Q Aspen 芯片通过长距离互连连接到单个硅载体芯片上。他们认为这是在现有制造技术的限制下的一种务实的选择。这种模块化的方法也可以为早期的 NISQ 应用提供更多的灵活性。

同样值得注意的是，Rigetti 使用了一种独特的超导量子比特方法，这种方法基于“参数门”的使用。他们寻求在 IBM 长寿命固定频率量子比特和谷歌可调谐量子比特提供的快速门之间找到一条中间道路。Frank Wilhelm-Mauch（OpenSuperQ 的协调员）在欧洲量子周上发表评论，指出了参数门方法潜在的未来吸引力。然而，Fact Based Insight 预计，OpenSuperQ 所构建的初始计算机将使用更接近谷歌的设计。

2020 年，Rigetti 获得由 DARPA 的 ONISQ 计划提供的 860 万美元资助，参与一个 1000 万英镑的项目帮助英国部署第一台商用量子计算机。

Wave 继续走自己的道路，专注于量子退火。这使 D-Wave 迅速扩大规模，瞄准早期客户机会。其最近推出的 Advantage 系统是一个重大升级，5000 个量子比特中有 15 个量子比特互相连接。但是，该技术的一个缺点是，它在理论上没有很好的途径来实施纠错，因此最终无法扩展到 FTQC。

据报道，D-Wave 经历了一轮艰难的融资，但迎来了一个有趣的战略合作伙伴——日本 NEC 在混合产品开发以及销售和市场推广方面都具有影响力。

芬兰的 IQM 是一家提供差异化产品的初创公司。IQM 将为研究机构和高性能计算中心构建现场量子计算机，并为企业客户提供协同设计方法。这与欧洲对技术主权的担忧相呼应，也与芬兰在低温系统（Bluefors）方面的领先技术及其合作伙伴在控制系统（Zurich Instruments）方面的专业知识相一致。

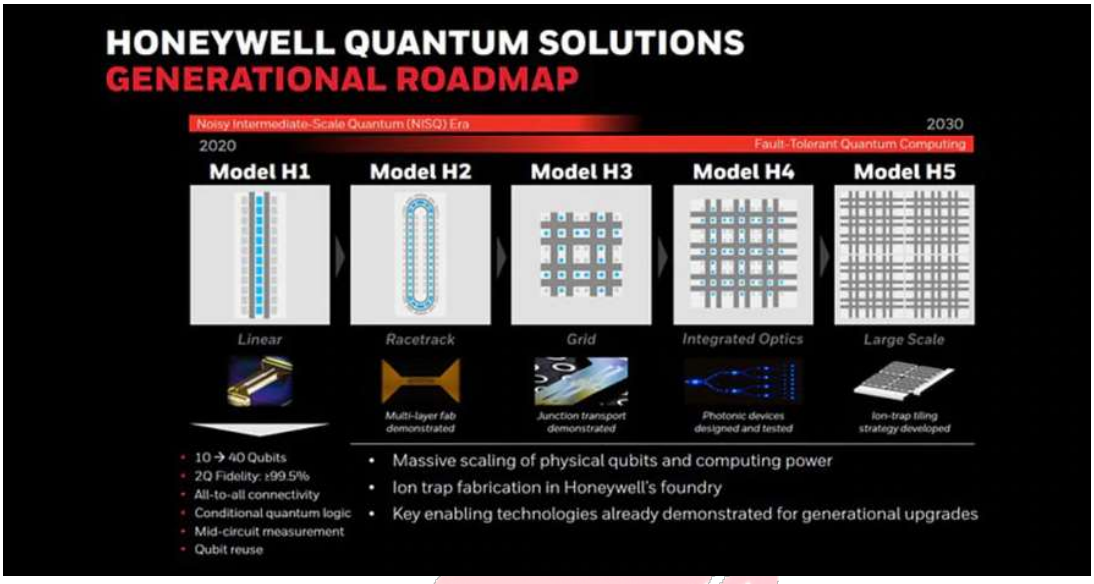
2020 年，IQM 赢得了 VTT 和芬兰政府的联合创新公开招标。这项耗资 2070 万欧元的项目将于 2024 年在芬兰交付一台 50Q 量子计算机。其他一些公司，比如最近与 Q-CTRL 合作的 Quantum Machines，也瞄准了这个研发市场，并且已经拥有了跨越 10 个国家的专业客户群。

总体而言，超导量子比特技术的一个优势是可以使用其他工程选择。但是，Fact Based Insight 认为，每家公司的具体方法将在商业上变得越来越重要。当每个人都希望扩大规模时，这些方法的扩展特征和挑战是不同的。重要的是，该领域的创新通常可以申请专利。如果参数门胜出，Rigetti 的专利组合将大放异彩；如果布线几何成为瓶颈，那么可以期望 IBM 的多层超导布线或 OQC 的 co-axmon 一跃而上；如果 Seeqc 的“数字” SFQ 控制技术可以像广告中所说的那样工作，预计其他公司也会被影响，因为它构建了自己独特的混合片上系统模块和特定应用量子平台。

二、进击的离子阱

量子在 2020 年的发展非常顺利。尽管 QV 是 IBM 率先提出的一种衡量方法，但是霍尼韦尔已经成为第一个用其 6Q H0 和 10Q H1 处理器达到 QV 64 和 QV 128 的厂商。有些人可能想，10Q 处理器怎么能声称自己和 IBM 的 27Q 处理器一样强大呢？但是，这恰恰凸显了离子阱研究者长期以来所阐述的两个优势：与超导量子比特方法相比，它有优越的连接性和更高的门保真度。这两个优势可以保证更高的 QV。霍尼韦尔处理器也是首款实现中间电路测量的处理器，进一步提高了灵活性。

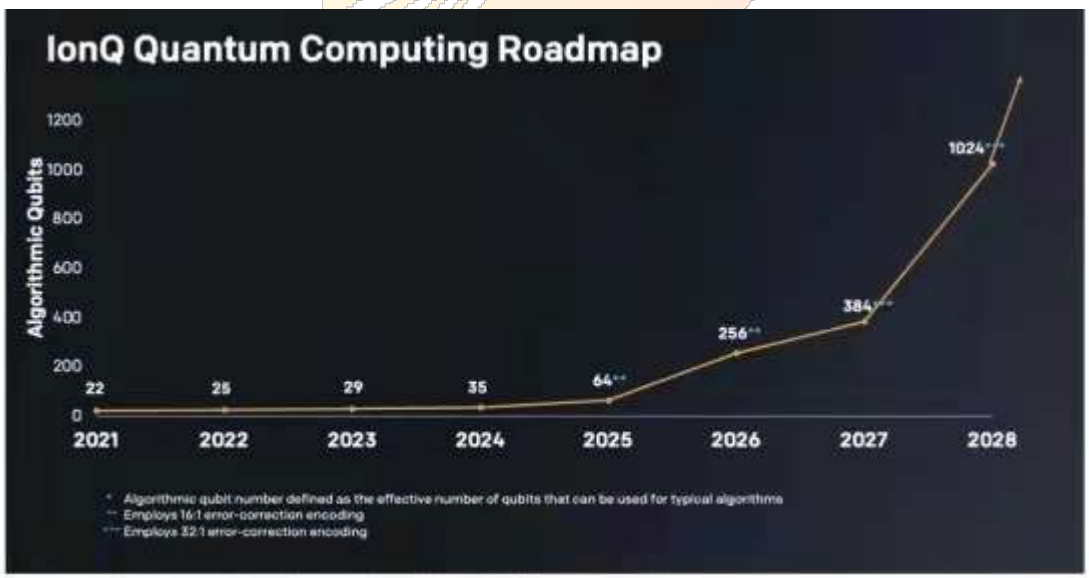
霍尼韦尔路线图（不同的量子比特布局）——2020-2030 年，H1（线性离子阱），H2（跑道布局），H3（网格布局），H4（集成光学元件），H5（大规模平铺）。



IonQ 宣布了一款 32Q 设备，他们希望获得比以前高得多的 QV，尽管他们现在更喜欢谈论一种新的衡量指标——算法量子比特（AQ）。

IonQ 路线图 - ——2021 年 22AQ、2023 年 29AQ、2025 年 64AQ、2026 年 256AQ、2027 年 384AQ、2028 年 1024AQ。错误纠正——2025 年 16：1、2027 年 32：1。

算法量子位比特（AQ）——IonQ 定义为可用于计算的有效量子比特的数量（注意：可用逻辑门深度仍有限）。在没有纠错编码的情况下，AQ = log 2（QV）。



Numbers shown are Algorithmic Qubits (described below). Credit: IonQ.

离子阱系统的一个缺点是，与超导量子比特相比，它们提供的门速度要慢得多（通常慢 100 到 1000 倍）。他们希望通过更长的量子比特寿命和更高的保真度来弥补这一点，从而减少纠错成本。

最近 Chris Monroe 团队的一个实验室演示（其设置与 IonQ 的设备非常相似）已经看到一个逻辑量子比特成功地从 13 个物理量子比特中编码。使用的 Bacon-Shor-13 代码无法提供与拓扑代码（例如表面代码或颜色代码）相同的长期可扩展性，但确实为有效错误率的中期改进指明了道路。

IonQ 相信，结合高保真的物理量子比特，这将足以比其他方法更快地实现量子优势。

对于离子阱系统而言，真正的长期挑战是再次扩大规模，尤其是在它们依赖精细调谐的激光系统来驱动其高保真量子比特门的情况下。就像超导量子比特方法不同一样，离子阱也不尽相同。

比如，奥地利公司 AQT，他们没有使用霍尼韦尔和 IonQ 使用的在超精细跃迁上定义的量子比特，而是使用在光学跃迁上定义的量子比特。虽然寿命较短（保真度稍低），但这种量子比特的工作波长是集成光子组件易于制造的波长，因此有望实现更容易的扩展。2020 年，这种集成设备在实验室中以这些波长进行了演示。这有望为更轻松地扩展该技术开辟道路。AQT 与欧洲量子技术（QT）旗舰计划、AQTION 合作，首次构建完整的“机架系统”。

其他离子阱初创公司的目光不再局限于激光驱动的门。Universal Quantum、NextGenQ 和 QT 旗舰计划的 MicroQC 正在寻求将远场微波门带出实验室，并应用到商业设备。投资者可能会特别注意，与激光驱动门的许多关键性能记录密切相关的 Chris Balance 和 Thomas Harty，已选择以自己的初创公司作为基础，建立近场微波门，如 Oxford Ionics。

离子阱架构通常使用模块之间的光子互连进行扩展。最近已经演示了更快的互连，但是似乎仍然是一个性能瓶颈。另一方面，Universal Quantum 已经证明他们的离子穿梭方法原则上可以提供类似于全连接的 QV。

三、云中的中性原子

中性原子量子比特在 2020 年继续突飞猛进的发展。它们与离子阱有许多相同的特性，它们的优点是中性原子可以被包裹得更紧密。这意味着可以更快地扩展到 1000Q 模块。

该技术又叫作冷原子，因为它使用激光冷却和高度真空来达到毫开（mK）的温度，远低于低温冷却的范围。

ColdQuanta 是采用这种方法的知名公司，已经推出了 QuantumCore 作为一个基本单元，以

瞄准许多量子领域的机会。它也是云上的量子物质系统 Albert 的基础。ColdQuanta 已经被 DARPA（美国国防高级研究计划局）选中，作为 ONISQ 计划的一部分，参与 1000Q 处理器的开发工作，该奖项的价值高达 740 万美元。

ColdQuanta 路线图——到 2021 年达到 100Q，到 2022 年达到 300Q，到 2024 年达到 1000Q。

其他选择中性原子的公司还有 QuEra、Paswal 和 Atom Computing 等。

四、长期使用的硅

2020 年，基于量子点的硅量子比特在实现其长期承诺的优势之一方面取得了重大进展。QuTech 和新南威尔士大学（UNSW）在 1K 的温度下用金属氧化物半导体（MOS）量子点演示了量子比特操作。这有望成为一个操作和扩大设备规模明显更容易的机制，尽管在这些更高的温度下，相干时间和保真度是否具有竞争力仍有待观察。

QLSI 是一项耗资 1400 万欧元的 QT 旗舰新项目，是推动该技术在欧洲发展的重要推动力。知名的参与者包括 CEA-Leti、CRNS 和 QuTech，以及已经活跃于这项技术的商业参与者和初创公司，包括 Hitachi Europe 和 Quantum Motion。目的是在 2024 年之前演示 16Q 设备，并评估向 1000Q +的扩展性挑战。QuTech 已经在 Quantum Inspire 云平台上拥有一个 2Q 硅量子比特处理器。

澳大利亚初创公司 Silicon Quantum Computing 一直是硅量子比特的早期推动者。2020 年，它宣布了其路线图的重点，放弃了 MOS 量子点，并加码了磷原子量子比特。这些设备使用超尖端制造技术，提供了超越传统 CMOS 技术的原子精度方法。

SQC 路线图——2023 年实现 10Q 原型，2030 年实现 100Q，2030 年代中期实现 FTQC。

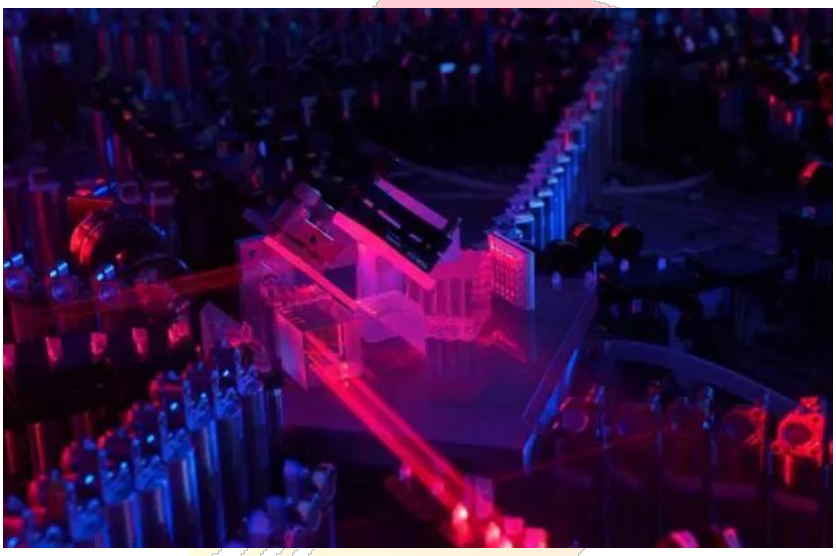
在描述 SQC 的制造技术时，Michelle Simmons（SQC 的创始人）指出不仅能够以原子精度设计量子比特，而且同样的技术可以在同一器件衬底内创建稳定、简单和原始的控制线路。今年，他们报道了硅量子比特实现迄今为止最低的噪声。从谷歌离开后，John Martinis 现在已加入 SQC，将开发具有超快速门和可扩展布线选项的设备。

2020 年，加拿大初创公司 Photonic Inc 发表了早期的研究，承诺给硅量子比特“军械库”增加一个重要的新工具。这有望改善基于硅中 T-centre 缺陷的光子的界面。

五、光子破坏者

中国的九章实验能够证明这一计算比迄今为止在任何其他平台上实现的计算都要复杂。九章通过实现一种被称为高斯玻色取样的算法来实现这一点，成功构建了 76 个光子 100 个模式的高斯玻色采样量子计算原型机。在 200 秒的时间里产生的输出样本，声称世界上最强大的超级计算机 Fugaku 需要 6 亿年才能实现。它的复杂程度大大超过了谷歌 Sycamore 最初的量子优势演示。

九章并非凭空而来。至少从 2006 年起，中国就一直在增加对量子技术的投资。潘建伟团队的专业知识是众所周知的，在 2019 年，他们首次实现 20 个光子 60 个模式干涉线路的玻色取样量子计算。最新的实验是一项令人瞩目的科学成就，并且是再次证明这个团队的科学与工程技术的杰作。



Anthony Laing（布里斯托大学）说：“相互干扰的光子数量激增令人震惊。从 12 个左右增加到 70 多个是巨大的飞跃，真的令人惊讶和印象深刻。我很高兴看到团队将可配置性开发到他们的设置中，以便与经典方法和硬件进行更好的比较。”

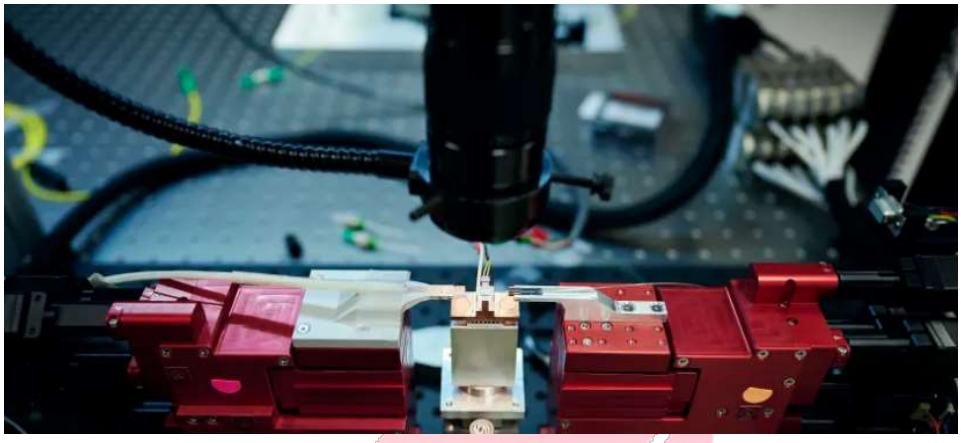
九章的意义不必过分解读。该设备当前的形式是不可编程的，它实现的是一种静态算法，而不是通用的量子计算方法。也许更重要的是，它是通过“传统”光学平台安装来实现的。所有的活性组件仍然是离散的。为了实现稳定的配置，需要进行许多手动调整。该方法在科学上令人兴奋，但对扩大规模提出了严峻的挑战。

西方国家多年来一直在追求集成光子技术，将其作为实现真正可扩展的光量子计算的一条有前途的途径。这要求（几乎）所有必需的组件集成到一个设备当中。主动可编程设备的演示可以追溯到 2015 年。

Xanadu 采用一种概念上类似于潘建伟团队的高斯玻色取样方法，并且已经提供了对可编程 8、12 和 24 模式处理器的云访问。

Xanadu 路线图 - ——2021-2023 并行的三个处理器系列：X 系列（当前）X40、X80；XD 系列（100%连通性）XD4、XD8、XD12、XD40、XD80；TD 系列（时域复用）TD2、TD3；在 5-10

年内增加到 100 万个量子比特。通过 GKP（一种基于玻色子的量子系统纠错方法）量子比特进行纠错。



QuiX 最近推出了 12 模式处理器。

QuiX 路线图 - ——2021 年 12 模式、2022 年 50+模式

PsiQ 已经为他们的计划筹集了 2.5 亿美元以上的资金，以在“数年内”构建一个通用的 100 万量子比特的设备，他们一直在使用标准的制造工艺与 GlobalFoundries 一起生产测试芯片。

PsiQ 路线图——100 万个量子比特，能够作为 100-300 个逻辑量子比特运行，据报道在 5-8 年之内。通过 FTCS（一种基于测量的量子计算纠错方法）进行纠错。

Duality Quantum Photonics 强调了专用的量子计算设备在 3-5 年内解决与工业相关问题的潜力，并计划在 2021 年推出其首个组件级原型。

集成光子学并不是西方的唯一想法。ORCA Computing 公司正在研发基于与光纤连接的分立模块组件的系统。ORCA 强调这种方法不是“孤注一掷”， 并承诺开发和重新配置的速度更快、成本更低。

六、扩大规模

在 IQT 欧洲大会上，Bob Sutor（IBM）总结了许多潜在采用者的看法：“从科学的角度来看，听到各种不同的量子比特技术总是很有趣的。但它们能突破 100 到 1000 量子比特吗？唯一的问题是可扩展性，有足够好的量子比特来解决你真正想要解决的商业问题。”

Michael Cuthbert（英国 NQCC 临时主管）表示：“现在决定赢家还为时尚早。有多种技术和多种扩展方法需要我们研究”。

大多数领先的硬件厂商都已经制定了自己的路线图。更重要的是，他们的硬件将花费大部分时间进行纠错。关于如何最好地做到这一点的争论已经与量子比特技术的争论交织在一起。

七、2021 展望

量子霸权——无论计算难度的争论最终结果如何，九章都会引起轩然大波。要注意这项技术能否可编程和可扩展。只有这样才能使它真正具有颠覆性。

QV——IonQ 对其新 32Q 量子计算机预期很高。实测性能真的会达到 400 万 QV 吗？(用 IonQ 新术语来说就是 22AQ)?

QV/s——量子体积可以用来衡量许多性能指标，但它没有办法衡量不同量子比特平台之间的原始门速度差异。预计超导量子比特社区将采取适当的措施进行反击，使他们能够展示自己的快速门。

量子比特数量——IBM 是否会第一个将 100Q+处理器与 127Q Eagle 一起放到云端？或者 Rigetti 会用 4x32Q 多芯片 Aspen 模块抢占、先机吗？我们将从谷歌的“100Q”设备中看到什么？注意同步 2Q 门保真度的趋势

逻辑量子比特——关注主要玩家的纠错演示，这表明他们正在迈向一个新的重要里程碑——操作逻辑量子比特。

中国——本源量子能否在云产品中增加 60 量子比特的悟源 2.0 设备?

欧洲——QT 旗舰项目 OpenSuperQ 预计将交付其第一台设备。距离 100Q 还有多远，对应的

QV 是多少？AQTION 将交付 50Q+设备；注意它的基于机架的灵活配置。

英国——Rigetti 正在英国建造一台基于超导量子比特的机器，容纳于牛津仪器公司最新的 Proteox 系列稀释冰箱之中。关注这台量子计算机可能公布的细节。

超导技术——观察初创公司的发展情况以及这种技术的新特点，如 SeeQC 和 OQC。特别注意 QCI 计划的细节。这是一支强大的队伍，但仍在暗中运作。他们选择支持的内容将成为他们如何看待未来扩展挑战的指南。

量子退火——注意未来 D-Wave 硬件计划的细节。Qilimanjaro 提出的“相干”量子退火器有什么细节。

离子阱技术——现有的领导者如霍尼韦尔和 IonQ 将由 AQT 推动。关注来自微波门技术初创公司的消息，如 Oxford Ionics、Universal Quantum 和 NextGenQ。

中性原子——2021 年，我们会看到 ColdQuanta 的 100Q 设备登上头条吗？尤其关注保真度。关注更多来自初创公司 QuEra、Pasqal 和 Atom Computing 的计划。

量子点——自旋量子比特原型通常基于硅衬底上的金属氧化物半导体或硅锗量子点。在过去的两年里，硅衬底上的锗量子比特已经取得了惊人的进展，包括由 QuTech 演示的 4Q 处理器。观察哪种变体将成为领先的量子点量子比特平台。

硅保真度——展示真正高保真的 2Q 门性能仍然是一个关键目标。关注 QLSI 财团透露的细节。我们会看到 SQC 或 Photonic Inc 开始赶上量子比特的高保真度吗？

光子平台——已经开发了这种技术的多种变体，每种都有不同的优势和劣势。绝缘体上硅(SOI)是最成熟的技术，并得到了 PsiQ 的支持。氮化硅(Si3N4)提供了一个强大的现有组件生态系统，并受到 Xanadu 和 QuiX 的青睐。这项技术的其他变化正在出现。注意这些技术中哪一项将在量子应用中脱颖而出。Duality 会选择哪一个作为它的起点？

专用设备——重视量子模拟器是欧盟量子旗舰的一个特点。注意 PASQuanS 和 Qombs 等项目的结果。通过 ATOS、法国电力和空客等公司，终端用户的参与度在这里尤其高。关注来自诸如 PASQAL、Duality 和 Bleximo 等初创公司的原型计划。

拓扑量子比特——2020 年经历了一次重大的挫折，对之前 TU Delft 关于马约拉纳准粒子的结果提出了质疑。继续关注相关争论。

控制硬件——R&D 市场将成为苏黎士仪器和 Quantum Machines 等控制专家的重要跳板。IBM、谷歌、英特尔和微软等巨头都将目光投向了距离量子硬件更近的低温 CMOS 控制硬件。Seeqc 正在开发自己的具有潜在颠覆性的“数字”控制技术。

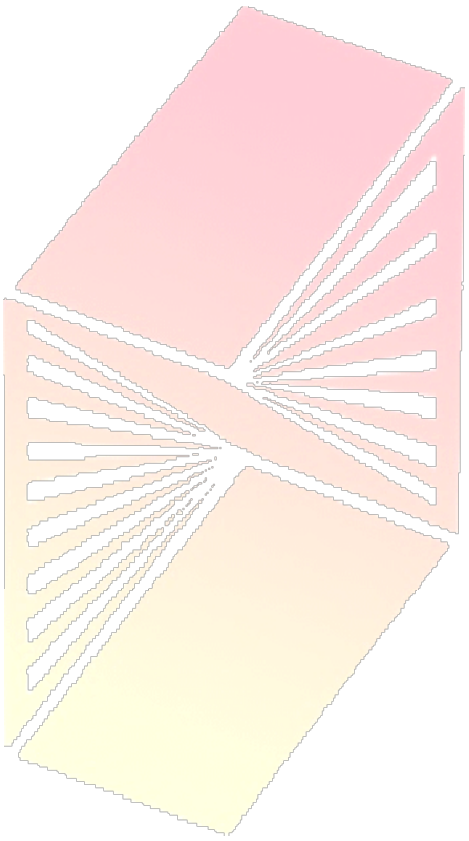
英国国家量子计算中心(NQCC)——关注 2021 年初多个技术领域的资助计划。

新的量子比特技术——AWS 对混合电声(electro-acoustic)量子比特感兴趣。Quantum Brilliance

正在研究一种基于金刚石 NV 的处理器。EeroQ 在寻找氦上的电子。注意这些和其他新技术平台的细节。

新代码——AWS 的混合电声量子比特不仅因其新的技术平台，还因其提出的“级联 cat 码”纠错方案而闻名。注意受这种方法启发的其他方案。

扩展，扩展，扩展——对于大多数设备来说，关键问题不是它们能做什么，而是它们展示了平台不断向量子优势扩展的能力。



第四章：2021 量子软件展望

IBM 继续主导着量子云平台的研发。这将是未来量子计算发展的关键，它可以处理更加复杂的运算，而且在竞争日益激烈的云计算服务市场上，如果推出量子级别的计算服务会占据绝对的优势。从长远来看，支持开发人员是传统软件行业的任务，但我们需要牢记，量子计算的底层技术与软件行业的本质是不同的，我们对待研发应该有彻底的革命精神。

在数字革命中，软件被认为是至关重要的商业竞争领域，许多人期望在新的量子革命中同样如此。各种各样的参与者正在研究不同的策略。如今，早期的量子社区和生态系统已经初步形成。

对于供应商而言，第一个挑战是如何进行合作以及参与哪一部分的合作？核心专业知识起着怎样至关重要的作用并且能在哪种规模下运用？在未来的量子软件价值链中，应该怎样捍卫自身的价值？

对于早期参与者，第一个挑战是如何让内部团队不断学习和研发？如何将这种基础理论知识转化为现实的量子路线图？如何避免在量子领域的进程中走弯路？

一、量子计算云服务市场升温

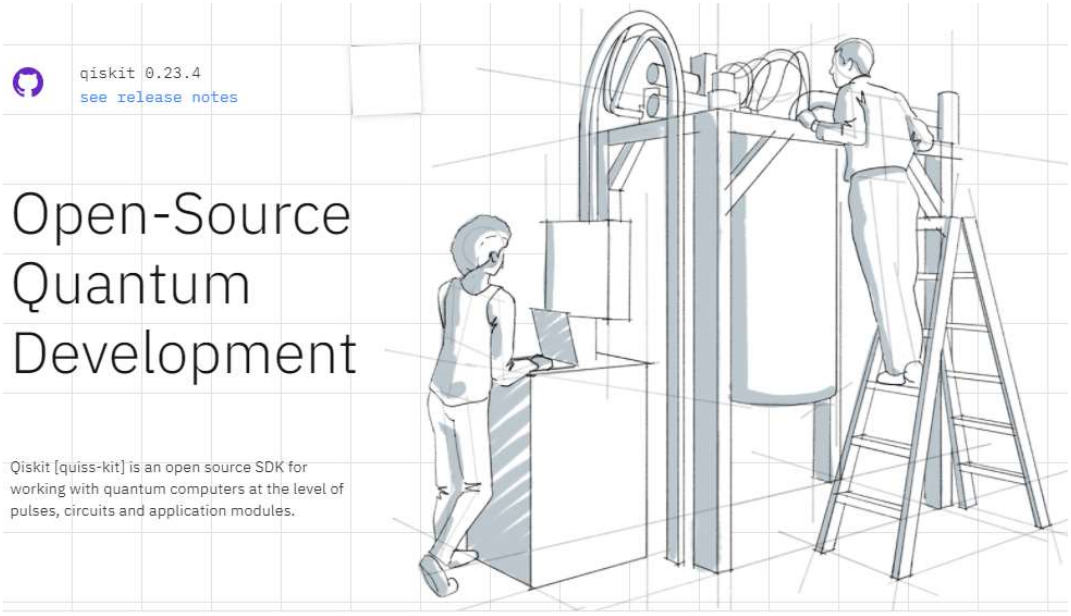
1. IBM Q

IBM 宣布实现其量子计算研发版图中的全新里程碑，过去四年中，IBM Cloud 上部署了 28 个量子计算系统，其中 8 个系统的量子体积达到 32。IBM Q Network 拥有 115 家客户、政府、初创企业、合作伙伴及高校成员。IBM Quantum Experience 注册用户数超过 25 万，用户定期通过 IBM Cloud 在 IBM 量子系统运行电路超过 10 亿。研究人员利用 IBM 量子系统已发表 250 多篇学术论文。IBM 用于商业的量子计算机服务 IBM Q 取得了阶段性的成功。

IBM Quantum Experience 于 2016 年启动，最初目标是通过提供一个简单的图形 Web 界面来建立知名度，用户可以在其中创建简单的量子程序，然后在早期的量子硬件上运行它们。IBM 在这一成功的基础上，构建了全球首个成熟的量子云平台，供科学和行业研究者使用。

IBM Quantum Network 合作伙伴包括戴姆勒、埃克森美孚、摩根大通、三星、高盛、埃森哲和波音等商业专业公司，成员总数超过 130 名。

Qiskit 是 IBM 的量子软件开发工具包，用于在脉冲、电路和算法级别处理噪声量子计算机：电路和脉冲级别的量子编程（Terra）、通用算法（Aqua）、错误表征（Ignis）和离线模拟（Aer）。



当其他竞争者开始建立自己的量子社区时,IBM 根据自身在早期阶段搭建量子社区的经验出版书籍。他们指出在不断发展的供应商生态系统中，可以提供与 Qiskit 兼容的库和工具，而不只是 IBM 硬件。

2. 来自竞争者的追赶

D-Wave 在 2018 年 10 月推出了 Leap 云平台，基于 D-Wave 量子退火处理器提供量子计算云服务。

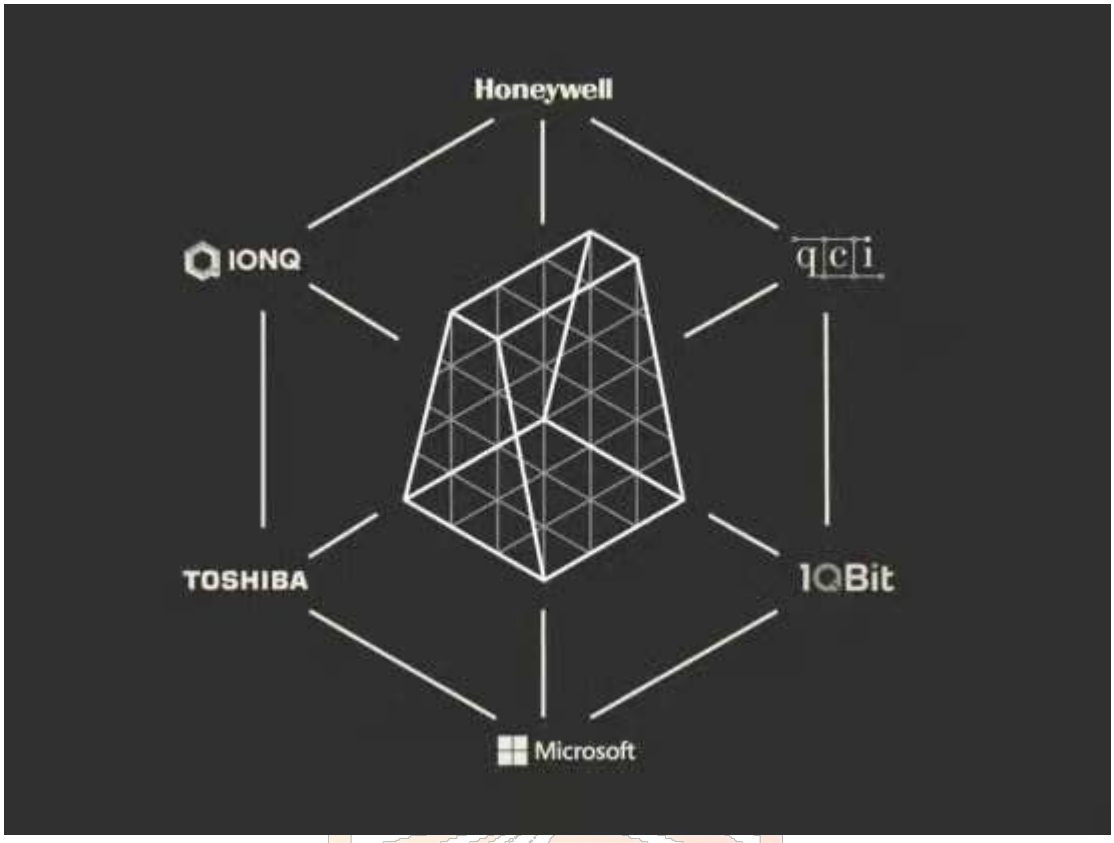
D-Wave Leap 预建整合开发者的集成开发环境，该环境使用最新的 Ocean SDK 设定与配置，并包括新的 D-Wave 问题检查工具与 Python 错误工具。并新增混合求解服务，可以支持自动判断应以量子或经典云数据来解决使用者所输入的问题,而且最多可支撑拥有 1 万个变量的复杂问题。

量子计算先驱 Rigetti Computing 推出了 Rigetti 量子云服务(QCS)——这是一个利用 Rigetti 的混合量子/经典方法开发和运行量子算法的完整平台。量子优势是使用量子计算技术解决重要或有价值的业务问题。最近，越来越多实力雄厚的量子公司开始投入量子云服务平台的研发当中。亚马逊 AWS 发布量子计算服务 Braket，此外，AWS 还将启动“AWS 量子计算中心”和“亚马逊量子解决方案实验室”，推动更多量子计算的合作。

Amazon Braket 于 2020 年全面上市，可在 D-Wave、IonQ 和 Rigetti 系统的量子处理器上运行算法。该服务具有自己的 Amazon Braket SDK，是一项全新的、完全托管的 AWS 服务。早期的蓝筹合作者包括大众、富达、安进和意大利国家电力公司，初创企业和学术合作伙伴包括 Rahko、Qu&Co 和 IQC。

微软的 Azure Quantum 在 2020 年上线。它承诺可以从霍尼韦尔、IonQ 和 QCI 以及 Toshiba SBM（用于模拟退火）中访问量子后端。量子开发人员可以使用 Q＃语言和 QDK 开发工具编写算法，然后使用三种量子计算机后端对算法进行评估（霍尼韦尔、IonQ 和 QCI）。这种资源整

合将使开发人员不接触量子硬件的底层物理原理，也可以编写和测试量子程序。



微软能够通过“Q Station”继续从事量子计算基础研究。AWS 也在努力赶超。

Google 一直保持对其先进硬件的访问权，但现在已启动了一项早期访问计划，以允许特定的外部人员访问其量子云服务。早期访问权限主要提供给美国学术和国家实验室专家。量子软件初创公司 PhaseCraft 是被邀请的唯一商业公司。

Google 的量子计算服务最初利用算法框架 Cirq 和自己开发的 OpenFermion 和 TensorFlow Quantum（一个用于混合量子经典机器学习的库），基于 Sycamore 量子处理器进行访问。Google 提供了自己实验的代码示例（ReCirq）和模拟器工具（Qsim），支持可认证的随机数生成。所有工具和库都是开放源代码，可连接到 Google 专有的 Quantum Engine 云服务。

总体而言，量子云服务平台市场参与者的增加反映出各公司技术专业人才的广泛笼络。想要打赢量子领域的硬仗，还需投入大量的资金。

二、教育的重要性

建立量子算法平台用户群的第一步是用户参与和教育。

2020 年的一大亮点是首届 IBM 量子编程挑战赛。比赛设置了四个任务供程序员试用其基于云的量子计算机，以扩展量子编程技能。

IBM 量子编程挑战赛：仅在第一个任务中，就有 1745 人参加，其中 574 人正确完成了所有任务。这在很大程度上是一次量子教育和社区建设活动。Fact Based Insight 认为，举办这样的活动是公司鼓励具备量子专业素质的员工开始从事量子之旅的绝佳方法。

面对竞争者，Google 也不甘落后。来自 Quantum Realm Games 的量子国际象棋有望成为 Google 量子云计划的一个成功项目。

量子国际象棋：新颖之处在于允许棋子进行“拆分”动作，通过结合叠加、纠缠和干涉的量子概念进行游戏，物理学家 Spiros Michalakis 在活动现场直播中解释说：“就像您在多重宇宙中玩耍，但在不同宇宙中不同的板块相互连接。”当不同的板块试图连接时，会发生量子测量，从而确定结果。

2020 年，Q2B 举办了首届量子国际象棋锦标赛。经过多轮比赛后，Aleksander Kubica 取得了胜利。

这是量子算法在经典游戏的有趣应用。量子领域需要一些方法来使不具备量子专业知识的人对量子计算结果与经典结果有所感受，领略到量子的魅力。量子国际象棋做到了这一点，甚至可以使参与者的教育程度降低到高中水平。中国科学家也已经沿着类似的思路开发了量子围棋。

另一个有趣的量子算法学习产品是 Q-CTRL 的 BLACK OPAL，它可以在光滑的仪表盘上可视化处理错误，最重要的是，可以帮助用户可以直观地查看噪声的影响并使用控件对量子计算机的电路进行重新编程来纠正错误。

在欧洲，QuTech 的 Quantum Inspire 量子云平台能够让所有人都能够访问量子计算机，而且所访问的量子计算机还是世界上第一个使用由可扩展自旋量子比特制成的量子处理器。该平台还提供对超导（Transmon）量子比特制成的处理器的访问。因此，用户可以测试量子算法并比较处理器的效果。

三、高性能模拟器

对于量子开发来说，高性能模拟是关键一环。随着要模拟的量子比特数量增加，量子模拟器的开发迫在眉睫。

IBM Quantum 支持一系列离线和在线模拟器。Google 的高性能开源量子电路模拟器 Qsim 已证明能在 111 秒内在一个谷歌云节点中以 14 栅极深度模拟一个 32 量子比特量子电路。像 Amazon Braket 和 Azure Quantum 这样的参与者非常重视他们灵活配置传统云硬件以满足用户需求的能力。Amazon Braket 提供完全托管的高性能张量网络模拟器（TN1），这种基于张量网络的电路模拟器可以支持高达 50 个量子比特的量子计算模拟。

Atos 是数字化转型的全球领导者，同时也是第一个成功模拟量子噪声的公司。其开发的量子模拟器 Atos 量子机器学习机（Atos QLM）被称为世界上性能最好的商用量子模拟器，该

模拟器将高功率、超紧凑的机器与通用编程语言相结合，使研究人员和工程师能够开发和试验量子软件。Atos 公司已在包括奥地利、丹麦、法国、德国、荷兰和美国在内的众多国家安装了量子学习机，量子模拟器能够模拟多达 40 个量子比特。

中国云产品目前强调研发量子计算模拟器。华为的 HiQ 2.0（出于监管原因仅在亚洲使用）最多可模拟 42 量子比特 。阿里巴巴的 AC-QDP 声称即使在 50 量子比特时也可用于某些应用。本源量子最近通过访问其 6 比特量子处理器之一（计划扩展到 24 比特，正在进行中）推出了基于真实量子计算机的云。

四、帮助量子企业的研发工作

随着越来越多的公司开始从事早期的量子计算研发活动，许多初创公司正在寻求为新生的量子应用软件开发提供合适的开发环境。

一些公司已经是量子计算技术专家，他们希望能够以最小的成本迭代运行并能够轻松访问的加速模拟器工具。

Zapata、QC Ware、1QBit 和 Strangeworks 均提供出色的量子产品。到目前为止，Zapata 筹集了 5700 万美元用于研发，而 QC Ware 则受益于 Q2B 会议抓住了研发的早期优势。

Orquestra——Zapata 的企业平台为其提供了灵活的工作流模型，以支持许多量子解决方案需要的混合经典/量子处理的多次运行。Orquestra 旨在设计、操纵、优化和运行量子电路。这些量子电路被通用化，可以在不同的量子计算机、模拟器和 HPC 资源上运行。

Orquestra 可以自动化和统一会分散专家注意力的数据处理任务，其中包括一个广泛的库，提供优化的开源（VQE、QAOA）和专有（VQF）算法。该环境允许用户将不同库中编写的模块组合在一起，包括 Cirq、Qiskit、PennyLane 和 PyQuil 等一些模块。

Forge——QC Ware 的产品侧重于研究如何将经典数据有效地加载到量子硬件上，以及如何从量子角度进行距离估计，它提供了二进制优化、化学模拟、机器学习和蒙特卡罗模拟，此外还计划在这些基础上构建针对行业的软件应用程序。Forge 数据加载器是一个有趣的功能，可以将经典数据最佳地转换为易于在机器学习应用程序中使用的量子态。其著名的客户包括 Equinor、空中客车、宝马、高盛、爱信和科思创。Forge 与 Amazon Braket 合作，并且现在也可以在 IBM Quantum 上运行 Forge 算法，Forge 的最新版本还包括用于 GPU 加速的工具。

Quantumcomputing.com——Strangeworks 是一家位于德克萨斯州奥斯汀的量子计算软件初创公司，他们的目标是：通过为开发人员、系统管理员和首席信息官们设计软件，实现量子计算。与 Amazon Braket 或 Azure Quantum 等环境相比，这家公司将开发环境作为中心，提供了主要的量子框架（包括 Qiskit、Q#、Forest 、Cirq、Ocean 和 Pennylane）中管理编程项目的能力。

五、未来的应用领域

真正的量子应用软件的出现还为时过早，但是初创企业已经在为这个未来市场定位。关键一点在于平衡量子算法的专业知识与深入的行业洞察力，与传统应用软件领域相比，后者可能甚至更为重要，建立可以与行业保持互动并繁荣发展的商业模式是一个挑战。

算法专家正在围绕客户进行试点合作，建立针对特定行业的工具和库。例如量子化学中的 1QBit QEMIST、CQC 的 EUMEN 和 HQS 的 QAD Cloud 。

其他公司则强调与基于传统 AI 和数据科学技术的协同作用。例如 Multiverse 中的 QDL 和 FS 中；药物设计中的 ProteinQure。同样，Qu&Co 强调了与 Schrödinger 的战略合作关系，Schrödinger 是当今使用的常规量子化学软件的领导者。

还有的公司则利用量子退火和量子启发算法来获取利益。例如 1QCloud 中 POLARISqb 和 1QBit。

剩下的则在强调其算法研发工作中的学术实力。这有助于确保政府资金用于尖端创新。例如 Phasecraft 和 BEIT。

在量子应用市场中，量子技术不应该太过炒作。

六、量子编译器

与传统的编译器相比，优化量子编译器是量子研发阶段的一大挑战。量子计算设备存在物理量子比特之间的有限连接，使得只能在有限的量子比特对上应用双门。现实世界中的量子设备是存在噪音的，但是可以研发一种用于表征大型量子计算机噪声的算法以解决这一问题。从技术上讲，我们实际上经常在谈论转码操作，因此互操作性是一个有用的功能。

t | ket〉是 CQC 的高性能量子软件开发工具包，t|ket〉目前支持在 Amazon Braket 和 IonQ 量子计算机上执行量子电路，以及在 Windows 操作系统上进行应用程序开发。制作成功的量子优化编译器具有强大的数学意义。它让研究人员、算法设计者和软件开发人员能够在可获得的最先进量子设备上构建和执行量子电路，从而获得最佳结果。

编译器市场中出现了几个富有前景的方向，都是建立在深厚的专业知识基础上，这些专业知识在许多情况下是互补而不是竞争。随着在早期在量子硬件上实施纠错代码的竞争日渐激烈，编译器创新又将迎来新的浪潮。

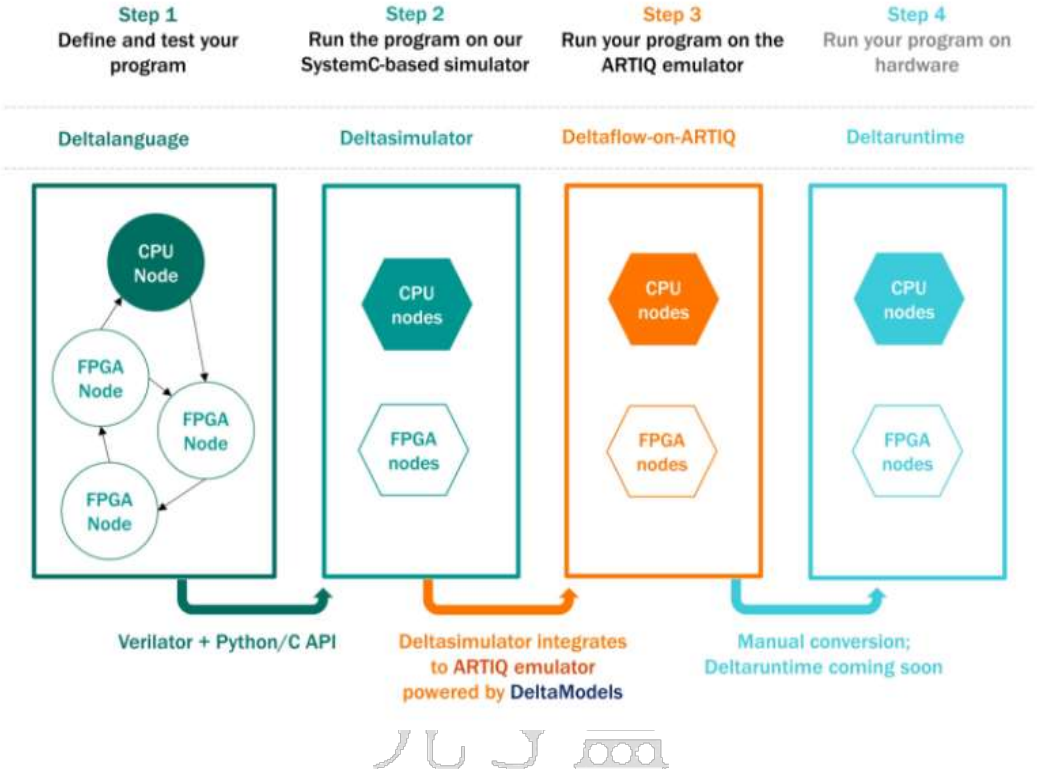
七、量子操作系统

量子软件行业的前景令人印象深刻，但是在量子计算机硬件高速增长的今天，如果没有操作系统，量子计算机的实用性将会大打折扣。

Riverlane 的 Deltaflow.OS 是一个新的全栈量子操作系统。由总部位于剑桥的量子计算软件开发商 Riverlane 牵头的财团从英国政府获得 760 万英镑（约合 6900 万 RMB）的拨款，用于部署高度创新的量子操作系统 Deltaflow.OS。

与其他旨在吸引早期用户的软件平台形成鲜明对比的是，Deltaflow.OS 解决了一个非常重要的问题——实现硬件和软件的交互，并充分利用量子计算性能。为此，它提供了加速开发、低延迟以及在应用程序和控制层之间进行灵活交互的潜力。

Deltaflow.OS：量子处理器通常由常规主机处理器驱动。在这两者之间，设想一个由全局和本地控制节点组成的网络。Deltaflow.OS 简化了将自定义代码获取到由 FPGA 实现的控制节点上的任务，强调了简化的指令集实现，这些实现更易于调试。这种方法有望缩短研发周期。它还使用分布式而不是分层的网络节点概念，并公开了整个量子计算堆栈的不同元素，这些功能有望最大程度地减少运行时的延迟。



Deltaflow.OS 现在已经发布了第一个版本，该版本与 ARTIQ（一种流行的离子阱控制系统）集成为“Deltaflow-on-ARTIQ”。这是该公司开发支持量子计算的技术的最新里程碑，标志着 Riverlane 朝着构建高性能、可移植于所有量子比特技术、可扩展到数百万量子比特的量子操作系统的目标迈出了重要一步。

Deltaflow.OS 与其他企业软件不兼容，但是它确实创造了巨大的价值。如今没有人知道量子计算领域将如何发展，但是在世界的某个角落，仍有各种不同的量子技术和初创公司在不断研发创造。

八、量子软件堆栈

尽管我们对量子硬件性能有不同的衡量标准,但我们仍然很少能解决怎样从云端到终端使用这些系统。QED-C 标准委员会主席 Tom Lubinski 指出:“许多用户都热衷于寻求某种东西,这些东西可以帮助他们决定将宝贵的时间和金钱投资于何处”。

从长远来看,许多人认为必须将多数开发人员的经验总结为一个简单易懂的结论。Google 前首席执行官 Eric Schmidt 在 Q2B 上发表讲话说:“随着技术的进步,从现在起的 8-10 年,人们将再次使用 Python 和 PyTorch 进行编写”。

九、2021 展望

云中的量子霸权——谷歌还没有成功地在 Sycamore 的常规(自动校准)运行中重复其量子霸权实验。谁是第一个让用户在云端实现量子霸权计算的公司?拭目以待!

云中的量子体积——量子体积是早期量子处理器能力的更全面的度量。如果离子阱产品能够在这里建立一个领先地位,那么对于提供访问的平台来说,预计会有一个大的突破。

云基准测试——关注标准“真正的问题”基准测试的发展。D-Wave 的新的 Qiskit 插件旨在使它能够轻松地在 Qiskit 支持的任何后端以及它自己的量子退火硬件上对一类重要的优化问题进行基准测试。

硬件无关平台——硬件无关的量子云平台(如微软 Azure)在财大气粗的科技巨头的支持下正在崛起。自有品牌全栈平台将如何适应?

参与度——IBM Quantum 在用户参与度和教育方面的领先地位令人望而生畏,不太可能很快被超越。我们是否会看到竞争对手在这一点上取得任何进展?

教育——关注专门针对教育市场的产品发布。BLACK Opal 2.0 预计将涵盖发现量子力学到执行算法,内容来自 Chris Ferrie(《给宝宝的量子物理学》的作者)。量子国际象棋大赛 2.0 承诺将包括量子解决方案的谜题。我们能看到谷歌 DeepMind 的一个 AI 对手吗?

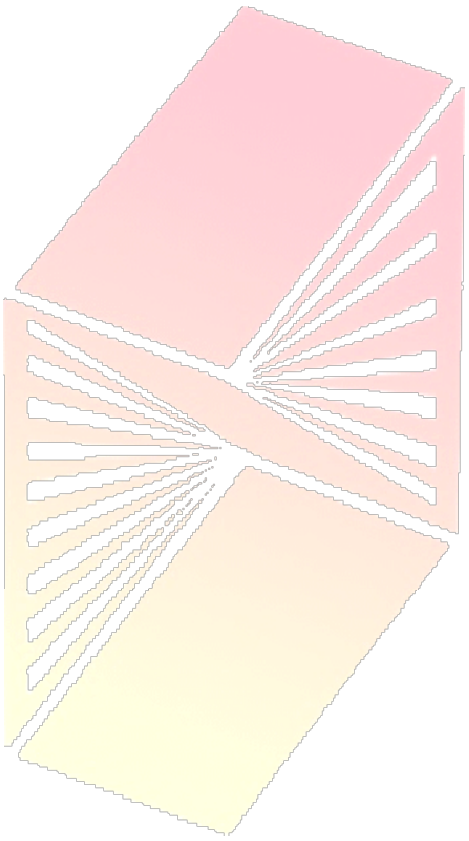
编译器——关注新的实用优化功能。

Horizon 公司——Horizon Quantum Computing 正在向早期用户开放其专有的编译器和软件开发工具。它有一个雄心勃勃的目标,即允许开发人员根据用经典语言(如 Matlab)编写的程序自动构造量子算法。这个平台是否允许更广泛的软件开发人员,在没有量子特定知识的情况下,将他们的技能带到桌面上?

量子网络——关注 Aliro Quantum 前两款产品 Q.Compute 和 Q.Network 的进展。这些会引起围绕量子网络的热议吗?

模拟器——高性能模拟仍然是理解、测试和验证量子软件的关键。注意优化的模拟器性能。

量子象棋 vs 量子围棋——中国大型企业和初创企业的量子云平台越来越多地寻求复制西方开创的用户参与之旅，比如量子围棋。



第五章：2021 量子算法展望

尽管目前已经取得了进步，但要在现在的量子设备上证明量子算法的优势仍为时过早。未来的大型量子计算机前景可观，但支出较大。即使拥有一百万个量子设备，若使用当前的量子纠错方案，对于量子计算机的使用效率而言也只是事倍功半。

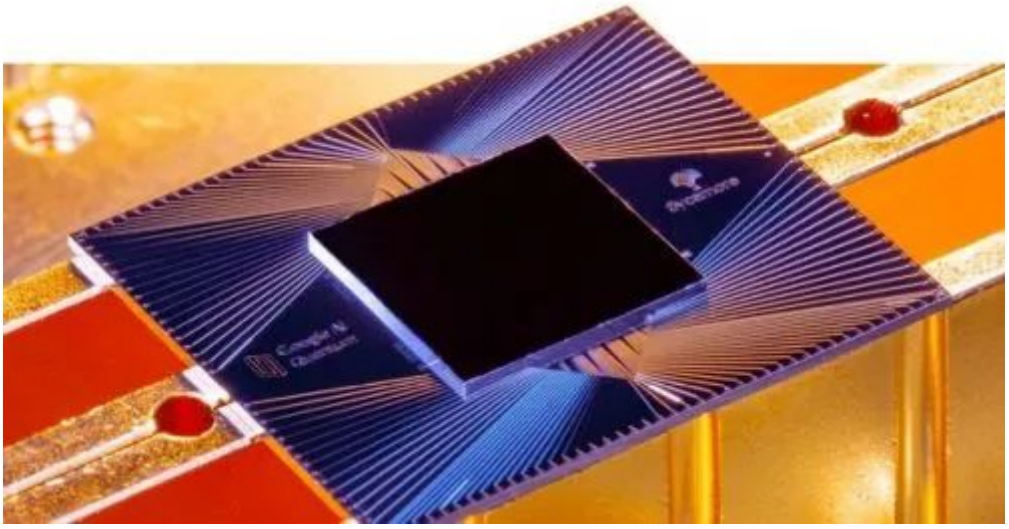
量子计算机能够非常轻松地解决世界上最强大的经典计算机需要漫长时间才能解决的复杂计算问题。早期的理论工作通常集中在容错量子计算机项目的研究上。在某些情况下，例如使用 Shor 量子算法（密码分析），Harrow Hasidim＆Lloyd（线性代数）和相位估计（量子化学），可以指数化提升运行速度。

但是，这种理想化的提速只是设想。近年来，人们的研究集中在量子启发算法如何用于 NISQ 设备上（例如 VQE、QAOA、QNN 和量子退火），而关于如何实现加速的理论基础并未得到官方的确立。

一、推动 NISQ 发展的量子优势

1. Google Sycamore 量子芯片

Google 的 Sycamore 量子芯片在 2019 年底大获成功，大大提升了量子计算性能。谷歌将“春季量子研讨会”作为其量子计算服务的亮点，量子研究成果令人印象深刻。Google 对 Sycamore 的研究集中在如何缩短量子计算的时长上，使其具有更高的计算性能。



VQE（变分量子特征值求解算法）用于模拟化学反应过程——分子级电子能量的 Hartree-Fock 计算上。尽管所执行的计算也可以在经典计算机上运行，但该实验构建了许多用于量子化学模拟的关键构建模块，为实现针对化学问题的量子计算铺平了道路。

化学公式（Trotterisation）用于模拟 8 位 1D Fermi-Hubbard 模型在材料科学中很受欢迎。令人惊讶的是，Google 能够成功实现量子算法所需的量子电路深度接近 500，比当前设备所期望的深度还要深得多。

在多次化学量子模拟的情况下，Google 展示了基于 N 表示性的错误缓解决策，极大地改善了实验的有效保真度。

Google 对于量子计算机是否能用于加速目前的化学反应量子模拟技术持保留意见。Ryan Babbush（Google）在 Quantum 2020 上发表讲话时总结道："下一代量子计算机是否能够解决经典体系中具有实际意义的棘手问题，仍未可知"。

2. 随机数和抽样

作为早期的量子计算服务产品，许多学者正在研究随机数。

可证明的随机数——Google 报告了通过质询和响应协议提供随机数的进展。这是 Google 第一个用于商业领域的量子设备，主要缺点在于成本较高。

可验证的随机数——CQC 展示如何使用现有的量子设备来实施基于云技术的 QRNG 服务。通过 Bell 测试，可验证产生的随机数来自量子源。beta 版 QRNG 服务已经可用于 IBM Quantum 网络。但是，在该协议中，用户仍然必须信任云服务提供商，因此该应用程序目前正在与其他拥有 QRNG 解决方案的公司进行竞争。

高斯玻色取样——九章在中国的头条新闻中提出了"量子优越性"这一定义，再次吸引了人们对高斯玻色取样的关注，并将其作为早期量子设备的候选算法。

Umesh Vazirani（伯克利）将经典密码学与量子领域进行结合，解决了"量子计算中最根本的问题之一，即如果你让一台量子计算机为你执行一个计算，那么你如何确定它确实执行了你的指令，甚至如何得知它是否做了与量子相关的事情。

3. 优化基准测试

从金融服务到物流再到制造业，优化算法是应用于实际案例的重要前提。早期的优化算法有 QUBO 和 QAOA 以及在传统硬件上运行的量子启发算法。

BBVA 已完成了一系列针对金融领域应用的前期项目，其中包括初创公司 Multiverse Computing 和 Zapata。BBVA 与 Multiverse 的合作是动态投资组合优化的一个经典案例，该投资组合现在已用于各种早期量子硬件的评估中，包括对 NISQ、量子退火解决方案和量子启发算法的测试。BBVA 的结果表明，量子退火解决方案和量子启发算法可以很好地解决投资组合问题。

在欧洲，汽车行业特别活跃，大众、宝马和零部件供应商博世等公司讨论了他们去年的经历。

优化算法再次被视为物流和制造运营中的关键机遇。

大众汽车已经着手研究一个现实世界中的问题,即在其生产线上如何最大程度地减少油漆车间的颜色变化。量子退火解决方案再次证明了其在此类应用中的有效性。

4. 离子阱使他们名声大噪

随着 IonQ 和霍尼韦尔推出的量子技术新设备,人们也在努力探索量子计算的具体实现路径。

QC Ware 在 IonQ 的 11 量子比特设备上展示了他们最近使用的质心算法和 Forge 数据加载器;

Zapata 建了企业级、量子赋能的软件，可以针对大量行业和用户，允许用户建立量子工作流，并在一系列量子和经典设备上自由执行；Rahko 展示 VQE 和 QML 技术的有趣组合，在霍尼韦尔 H50 量子计算机上发现了 2Q 和 4Q 分子的第一个激发态。

重要的是,像传统的机器学习一样,通过反复试验来进行研究的能力正是该领域的学者所不可或缺的。

5. 关键步骤

霍尼韦尔架构的关键特征之一是可在电路中间测量单个量子比特。从中期来看，所有设备都需要将此作为实现量子纠错的关键步骤。

Grover 搜索算法是量子计算中的一个重要算法，由于此算法需要非常大规模的容错量子计算机和 QRAM 技术来实现，因此在早期量子处理器的研究中它经常被忽略。但是，量子初创企业 BEIT 已成功使用中间电路测量技术展示了 Grover 算法的优化版本，从而在霍尼韦尔 6 量子比特 H0 离子阱设备上进行了搜索。

CQC 则演示了在使用 VQE 查找 H3 的基态能量时，如何通过增强物理对称性来成功地使用中间电路测量来减轻错误。

CQC 已利用霍尼韦尔的设备执行中间电路测量的能力来实现以测量为基础的量子计算(MBQC)。这是大多数当前设备中使用的电路模型的替代方法。实验证明，霍尼韦尔设备能够成功运行 172 次 CNOT 门和 105 次测量。正如 Ross Duncan（CQC）解释的那样，ZX 演算可用于在基于电路和基于测量的方法之间切换，这开辟了混合模型编译的可能性。

量子比特的中间电路测量复位是霍尼韦尔独有的技术,其他使用离子阱方法的量子计算公司也在试图复制该技术。霍尼韦尔实际上能够减少某些操作所需的量子比特数。

二、量子研究的成果

越来越多的因素促使量子专家和行业的先行者在 2020 年聚集在一起进行交流和讨论。

2020 年，由于 COVID-19 危机，诸如 IQT 纽约、IQT 欧洲、Quantum.Tech 欧洲、欧洲量子周、Q2B 等主要活动均在线上举办。但这些活动仍然向我们展示了量子领域的最新成果。

1. 模拟量子化学和材料科学

IBM 希望量子计算机可以在各种大型应用领域提供帮助，尽管对算法实施的计算机规模暂未可知：

改进固氮工艺以生产氨基肥料；
新型催化剂，可使二氧化碳更有效和更具选择性地转化为碳氢化合物；
用于锂-空气电池的新型电解质能够承受数千次充电循环；
可抵抗多重耐药细菌菌株的新型抗生素出现。

Quantum Benchmark 公司将材料科学（以及使用先进材料的行业）列为第一个可能从量子算法中受益的领域。这些材料本质上属于量子系统，因此通常有机会将我们的量子设备中的噪声转化为我们需要的部分。

根据经验，要模拟的一个电子轨道需要一个量子比特。因此，使用 100Qubit+设备似乎可以达到需要的效果。启发式变分路径是一种可能的方法，但是对于其具体应用仍在研究当中。

2. 优化金融、物流和制造业服务

在世界范围内，已有 20 多家金融机构在量子计算方面有所建树。高盛和摩根大通是 IBM Quantum Network 的合作伙伴。他们，发现将 1%的算法优势应用于商业领域能够产生显著收益。但是，算法实现仍存在一定的问题。

在 2020 年，高盛、摩根大通、巴克莱、BBVA 等公司一直在商讨他们正在进行的早期量子研究工作，并确定优先的研究领域，主要是金融投资组合优化和用于对金融衍生工具定价的蒙特卡罗技术。

算法也很重要。QC Ware 指出，他们开发的蒙特卡罗算法可打开量子算法应用于未来 5-10 年的金融行业应用程序的市场。

在欧洲，汽车行业特别活跃，大众、宝马和零部件供应商博世等公司讨论了他们今年的经历。优化算法再次被视为物流和制造运营中的关键机遇。

欧洲以特殊用途的量子装置（量子模拟器）而闻名。其中，与终端用户的互动是关键要素，也是量子技术旗舰计划的最终目标。

作为 PASQuanS 项目的一部分，法国电力集团正在与 Atos 合作，着眼于优化电动汽车的智能充电：最大限度地减少充电时间和充电站数量，同时也对提高能源效率产生影响。

3. 机器学习

许多人认为 AI 和机器学习是量子计算的关键。量子计算的未来，就像量子状态本身一样，仍然是不确定的。但量子计算的前景是光明的。

IBM 的最新理论工作首次证明，即使仅访问经典数据，我们也可以在某些受监督的机器学习应用程序中实现指数级加速。

QC Ware QC Ware 开发了两种类型的数据加载器，即并行数据加载器和优化数据加载器，它们都将经典数据转换为量子状态以用于机器学习应用，而且还可以使用一种优化的距离估计算法。

Matthias Troyer（微软）提出一个普遍的观点，为避免“输入瓶颈”，我们应该着眼于“小数据，大计算”。例如，CQC 成立了一个团队来研究量子自然语言处理的相关问题。

Hartmut Neven（Google）发明了另一种独特但微妙的量子机器运行原理。迄今为止，量子机器学习的大部分成功的实验都采用了一种不同的方法，那些实验里量子系统不仅只是模拟了网络；它们本身就是网络。每个量子比特代表一个神经元。尽管缺乏指数化的力量，但是这样的装置可以利用量子物理学的其他特性。

4. 掌握量子研发技术

空中客车公司是一个寻求早期量子研发的典型例子。“空客量子计算挑战赛” 提出了从简单的数学到飞行物理学，五个不同类型的问题。空客公司邀请了全球 36 个量子计算团队超过 800 位研究人员，从 1000 多个提案中筛选出 36 份完整提案，其中有 5 份进入入围名单。

空客量子计算挑战赛冠军——Machine Learning Reply 是领先的系统集成和数字服务咨询公司。他们的目标是在不断增加的飞行限制（例如有效载荷重量、重心和机身剪切极限）下优化飞机的装载配置。该方法在 D-Wave 量子退火机和经典求解器上运行 QUBO 算法，并通过数学建模（在注重安全的航空航天应用中的重要考虑因素）验证结果。

量子计算真正发挥作用还需要时日。空中客车公司已在整个量子领域建立了强大的知识网，也使空客量子研究团队对量子算法的研究有了更深的理解。

三、一百万量子比特的作用

一台能求解且有实用价值的超导量子计算机需要有上百万个量子比特，并且可以访问诸如 QRAM 和快速互连之类的资源。随着越来越多的硬件描述了针对“百万级量子比特”纠错量子计算机的路线图，自然就产生了一个问题——我们应该怎样做出这种规格的设备呢?

Google、微软和其他专家组也一直在积极研究其中的细节，思考该规格的设备如何实现。

优化问题——通常，这种类型的工作假设物理 2 量子比特门保真度可以提高到 99.9%（有时是 99.99%）；使用表面代码以大约 1 微秒的循环时间执行纠错；添加了 Toffoli 门来完成门设置，需要将机器的很大一部分用作优化的“神奇工厂”。

素数分解——2000 万量子比特，运行时间为 8 小时；

模拟 FeMoCo——400 万量子比特，运行时间为 4 天；

模拟二氧化碳的催化剂——400 万量子比特（4000 逻辑量子比特）和几周的运行时间；

模拟超导体——100 万量子比特和几小时的运行时间；

在 Fermi-Hubbard 模型中模拟材料——20-70 万量子比特和几天的运行时间。

1. 二次加速是否足够

Matthias Troyer 阐明了一个问题：实现这一规格将会存在一些严峻的挑战。

十个数量级——在目前的架构下，量子计算机的计算速度不比经典计算机快，且投入较大。量子计算机旨在通过使用量子算法提高计算运行速度，打败经典计算机。

目前在实现量子计算指数级加速方面没有理论上的难题。但是，在量子算法仅提供平方加速的情况下，存在一定的困难。

那么 Troyer 指出，量子计算机存在一段不必要的较长的运行时间。将算法改进以下，将能使量子计算设备的优势增加。

谷歌和其他公司在技术论文中提出了同样的观点。平方加速似乎不足以在基于当前前端运行架构的容错量子计算机上提供足够的运行能力。

这是一个大问题。Shor（密码分析）和相位估计（量子化学）等算法拥有对经典算法进行指数级加速的潜力。但是 Grover 算法仅做平方加速。

2. 寻求更好的加速

容错量子计算机前景广阔，但其功能仍然有限。大多数专家都接受了 Aaronson Ambainis 的猜想，即尽可能在某些结构上达到量子的指数级加速。

众所周知，绝热量子计算在原理上与基于电路的模型具有相同的计算能力。但是，尚不清楚随机哈密顿量的量子统计系统是否可以支持指数级加速。2020 年的工作表明，在某些情况下这是消除未来量子退火技术道路障碍的步骤之一。

Google 和 Troyer 的工作指出算法的前景，即提供多项式加速的算法比平方更具有优势，但即使是 Scott Aaronson，目前也无法研究出真正能应用到现实中的量子算法。

Harmut Neven 在 Google 的量子研讨会上总结道：“相对于传统计算机，量子计算机的计算能力正在以双重指数的速度迅速发展，但研究这一算法仍需要时间。”

四、2021 展望

量子性的证明——我们会更容易看到基于 PQC 陷门(trapdoor)的量子优势实验吗?

可认证的随机数——谷歌会使用其新的量子设备之一来推出远程可认证的公共随机性服务吗?

谷歌早期访问计划——谷歌目前正在将其平台的访问权限扩展到外部团体。第一波将由美国学术机构主导，物理模拟专家 Phasecraft 的加入引人注目。注意其他被选中的组织。

IBM Quantum 合作伙伴——包括戴姆勒、埃克森美孚、摩根大通、三星、高盛、埃森哲、JSR 和波音在内的蓝筹合作伙伴对 IBM Quantum Cloud 的扩张表示欢迎。

D-Wave——除了具有 5000 个退火量子比特和 15 路连接的新硬件外，D-Wave 现在还推出了扩展的混合解算器支持。注意可以解决的问题大小的影响。它的蓝筹客户会将量子应用程序投入日常业务使用吗?

新的量子联盟——高规格的离子阱处理器为探索 NISQ 算法提供了新的机会，NISQ 算法经过调整可用于高保真度、高连接性和中间电路测量。关注围绕 AWS Braket 和 Azure Quantum 新的量子联盟。

NEASQC——这一新的价值 4.7 欧元的 QT 旗舰项目将针对 NISQ 使用案例，与阿斯利康、法国电力公集团、HSB、Tilde、道达尔以及量子软件公司 Atos 和 HQS 等密切合作。注意工作的细节。

药物发现挑战? ——大型制药公司能否效仿空客的做法，加快构建自己的量子路线图?

科学的早期应用——基础科学研究中的应用成为早期应用日益突出的焦点领域,特别是量子机器学习。

NISQ 错误缓解——创新可能是早期商业应用能否通过 NISQ 设备实现的最重要驱动力。注意开发标准分层技术的工具箱。

不同的 FTQC 规格——FTQC 需要在不同的量子比特技术之间权衡。需关注为高规格应用程序提供所需资源的详细估计的工作。注意较慢的门速度与减少的纠错开销之间的相互作用。

第六章：2021 量子互联网展望

需采取行动，应对未来量子计算机可能存在的安全威胁。幸运的是，新的加密技术——量子抗性数字签名有望保护企业的系统安全。要了解基于量子物理基本原理的量子密码，就有必要先了解其安全性的保障以及该领域的长期发展方向。未来的趋势是，通信系统将变为通过量子纠缠交换连接在一起的量子互联网。

量子计算机将对商业和社会产生许多积极影响，但现在并不为世人所了解。当量子计算机升级到一定程度时，它将能够打破当前网络安全所依赖的公钥加密系统。更糟糕的是，量子技术能解密当前被拦截和存储的各种数据。

目前，学术研究正在迅速跟进，以填补技术发展带来的新漏洞。包括基于数学原理的后量子密码（PQC），以及基于物理学原理的量子密码方法，尤其是量子随机数生成器（QRNG）和量子密钥分发（QKD）。

但是，要了解这一迅速发展的行业，我们还必须研究一种更为重要的未来技术形态——量子互联网。

一、措施

未来的量子计算机所构成的威胁不应与网络安全的日常防火墙相混淆：

Michele Mosca（IQC 和 evolutionQ）：“这是我们在此之前从未面临的威胁。”

Eric Schmidt（前 Google 首席执行官）：“我强烈建议企业现在就采取行动。我们知道各国已经在着手准备。他们计划十年后能突破现有难题。”

John Prisco（安全量子和行业资深人士）：“ COVID-19 危机意味着，2020 年将是错失准备抵御量子威胁的一年”。

如今，多家知名量子硬件公司都制定了十年内生产出拥有一百万量子比特处理器的未来路线图。严格来说，此类设备可能仍然不足以打破我们目前的互联网标准（在 8 小时内达到 2000 万量子比特的估算）。而且，这些计划不可能一帆风顺。

2035 年及以后我们仍有极大可能受到量子互联网安全的威胁。但是，不断更新的量子纠错技术仍有潜力解决这一威胁。量子技术可能像曼哈顿计划造出原子弹那样改变世界格局。

Fact Based Insight 建议，企业需要一个“合理的最坏情况”日期，并以此为界做好应对准备。

二、后量子加密时代即将到来

自 2006 年以来，科学家一直在开发能够抵抗量子计算机对现有密码算法攻击的新一代密码算法。自 2016 年以来，该方法已通过 NIST 的评估，新的密码算法基于量子数字签名（QDS）和密钥封装机制（KEM）。

通常我们需要通过链路控制协议进行初始身份验证，交换加密密钥，然后再进行消息加密。今天，我们可能会使用 RSA 2048 + ECDH 256 + AES 128 构建公钥密码，在量子互联网时代，我们需要升级到 PQC DS + PQC KEM + AES 256 加密算法。

NIST PQC 评估——第一轮共有 69 种候选算法同时满足最低验收标准和提交要求，其中 21 种遭到破坏或受到严重攻击。NIST 选择了 26 种算法进入第二轮进行更多分析，其中 8 种遭受了攻击。到 2021 年，第三轮将完成对 7 个决赛选手的评估。标准草案预计在 2022 年发布以征询公众意见，最终草案将于 2024 年发布。

现在 NIST 的决赛入围者已经出现，我们可以更清楚地了解中期 PQC 领域中可用的工具。

公钥加密和密钥建立算法决赛入围者：CRYSTALS-KYBER、NTRU、SABRE 和 Classic McEliece。前三个是基于格的方案，提供了良好的安全性，是公钥加密/KEM 和数字签名方案中最有前途的通用算法。NIST 最终将选择一个作为标准。

Classic McEliece 是一个基于代码的 KEM，它有一个非常大的公钥，但在所有竞争的 KEM 中，它的密文是最小的。重要的是，McEliece 已经是一个众所周知的构造，40 多年来，它在攻击上只有渐进式的改进。

数字签名决赛入围者：CRYSTALS-DILITHIUM、FALCON、Rainbow。同样，前两个是基于格的方案，NIST 最终将选择一个作为标准。Rainbow 是一种多变量签名方案，使该方案面临更多的密码分析技术，但密钥尺寸非常大，使其不适合用作通用签名算法。

NIST 评估过程进展顺利，并正在计划中。 令人欣慰的是，尽管早有忧虑，但我们认为 PQC 能抵抗来自量子计算机的攻击。

三、现代量子密码学

1. 量子随机性

随机数是几乎所有密码系统的基本组成部分。QRNG 是一款超小型量子随机数生成器芯片原型。ORNG 已经被用于一些新兴的科技产业商品中。

IDQ 及其战略合作伙伴 SK 电信在 2020 年通过在三星手机上搭载小型 QRNG 芯片而引人注目。IDQ 还签署了越南智能手机制造商 VinSmart，并暗示其他手机制造商将很快效仿。

三星 Galaxy A Quantum——定制版三星 Galaxy A71 5G 在韩国推出，这款智能手机搭载了 IDQ 的 2.5mm 2 QRNG 芯片，用于增强 SK 电信提供的识别、支付和加密货币服务的安全性。

国家计划大力支持这些技术研发。IDQ 和 Quside 受益于量子技术旗舰项目的帮助，致力于研究如何使芯片更加便携，同时，KETS 也从英国 NQTP 项目中受益。

2. 量子密钥分发

量子技术还可以用于在两方之间安全地共享加密密钥。QKD 应用到量子力学的基本特性(如量子不可克隆性、量子不确定性等)来确保任何企图窃取传送中的密钥都会被合法用户所发现，这是 QKD 比传统密钥分发所具有的独特优势。

QKD 的优缺点——量子密钥分发的安全性基于量子力学的基本原理，而传统密码学是基于某些数学算法的计算复杂度。传统密码学无法察觉窃听，也就无法保证密钥的安全性。QKD 只能在传输时受到攻击，因此可以用来提供独特的持久安全保证。它的主要缺点是需要额外的硬件以及成本。在早期不成熟的量子设备中，密钥速率不高，而且范围必须限制在 70-90km，才能使用受信任的节点来进行中继协议。

现在，越来越多的公司以盈利的模式提供 QKD 系统。

国盾量子为迄今为止全球最大的运营网络提供硬件服务。目前正在扩展 2000 公里京沪干线，并建设 5500 公里的延长线。已经完成了合肥和武汉之间 700 公里的横向干线建设，另外还有 360 公里的在建工程和 2200 公里的拟建工程。

国盾量子在 2020 年上市最高涨幅一度超过 10 倍，涨幅达到 924%，这反映出广阔的市场前景以及政府对量子技术的积极态度。

IDQ 及其战略合作伙伴 SK 电信已在韩国部署了 QKD 试点，其中包括 SK 电信的 LTE 和 5G 网络首尔至大田段，以及韩国电力公司的电力网络 40 公里段。他们签署了建设 2000 公里 QKD 网络的合同，该网络为韩国 48 个政府组织提供网络服务。

东芝宣布即将部署商业量子密钥分发（QKD）平台，到 2035 年，有望突破 200 亿美元的市场份额。东芝的研发团队也非常强大，其研究小组在剑桥提出新的 TF-QKD 协议，承诺将实际的 QKD 扩展到“城际”距离，达 500 公里。

东芝估计，到 2035 年，QKD 市场将增长到约 200 亿美元，该公司的目标是到 2030 年占领 25% 的市场（约 30 亿美元）。同时，东芝欧洲公司与英国电信合作，在英国进行了量子安全网络的首次工业部署。

在欧洲，EuroQCI 计划包括 25 个欧盟国家和欧盟委员会、欧空局，其目标是建立泛欧安全的量子通信基础设施。OpenQKD 已在欧洲建立了 14 个测试中心。这些不仅包括电信骨干网和云数据中心等核心领域，还包括智能电网，电子医疗和电子政务等应用领域。

在过去的两年中，Quantum Xchange 推出了产品 Phio QK（多点 QKD）和 Phio TX（一种提供带外和 PQC 密钥的嵌入式解决方案），以用于服务纽约金融、电信和政府部门。

四、过去的争论

多年来，数学家和物理学家就 PQC 和 QKD 各自的优点争论不休。美国国家安全局和英国 NCSC（英国政府通信总部的一部分）在 2020 提出了他们的见解。两者都对 QKD 在现实世界的安全系统中的应用提出了质疑。NSA 强调了对早期 QKD 系统的漏洞的关注，而 NCSC 将重点放在整个协议栈中的身份验证协议上。

QKD 社区礼貌地回应了公众的争议，但仍有许多物理学家在私下提出不满，指出这些组织都是数学主导的 PQC 的坚定支持者。另一方面，太多以物理学为主导的小组都忽视 PQC 本身作为新技术的优点。

PQC 显然是我们现在可以采用的常规互联网和普通业务应用程序的首选选项。但是当需要更高级别的安全性并且产生一定的额外成本时，PQC 和 QKD 在分层防御中也显然是互补的。

QKD 有其独特的优点，只要不破坏初始密钥的形成，就没有机会对其进行攻击。实际上，实时 PQC DS 技术非常适合 QKD，可以形成优异且灵活的总体协议，同时增强其安全性。

五、现在的争论

最近，量子领域的技术环境发生了重要变化。政府已认识到建设未来量子互联网的核心任务是从目前的量子革命中找到其中的经济优势所在。

中国和英国的量子技术计划一直强调量子网络的重要性。欧盟的量子技术旗舰计划已将“在欧洲建立量子互联网”作为其长期战略目标。美国于 2019 年发起了自己的国家量子计划。在 2020 年，发布美国量子网络的战略构想。最近，英国政府的战略支出也将量子加密技术投资列为重点。

六、量子纠缠

量子互联网的基本资源是量子比特和量子纠缠。多个量子比特的相干操纵和纠缠态制备,是量子计算的最核心指标。

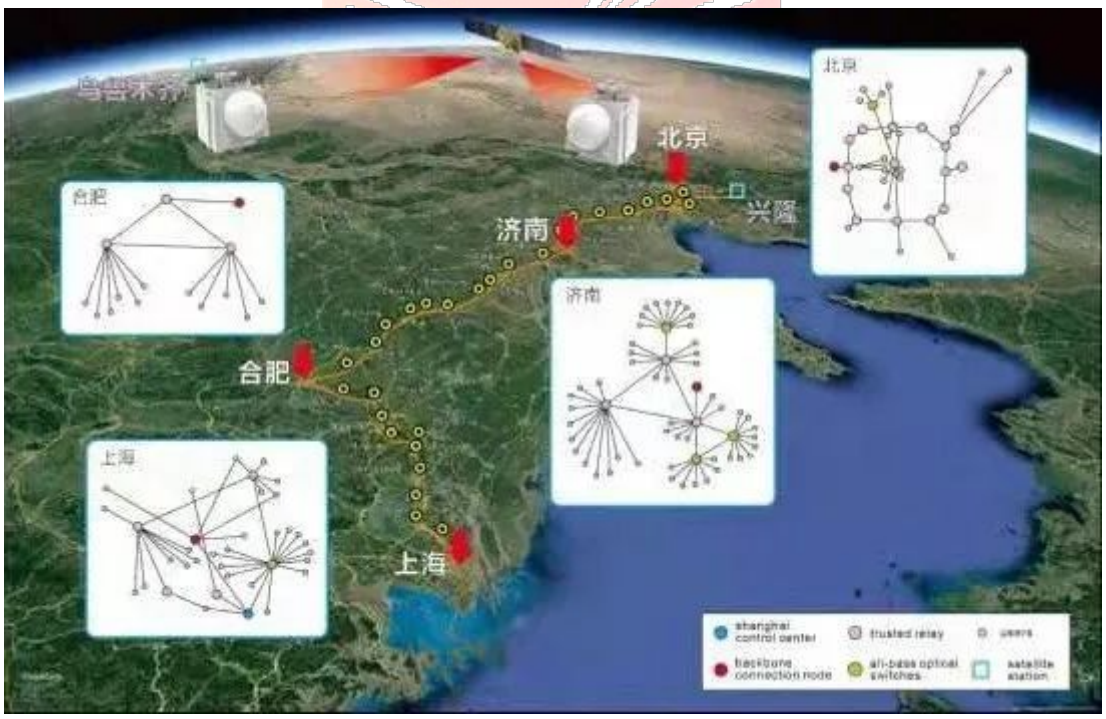
在量子力学里，纠缠是指当几个粒子在彼此相互作用后，由于各个粒子所拥有的特性已综合成为整体性质，无法单独描述各个粒子的性质，只能描述整体系统的性质。量子纠缠是一种纯粹发生于量子系统的现象；在经典力学里，找不到类似的现象。

目前最关键的挑战是如何根据自身需要在网络节点之间产生纠缠。虽然这最初是一个科学探究的问题，但现在却变成了一个非常现实的实际应用的挑战：如何将其扩展到可以共享纠缠的系统和范围；如何将纠缠作为网络资源进行管理？

七、太空领域

利用光纤网络实现量子信息传输时，卫星连接解决了地域限制的问题。

中国的“墨子号”卫星于 2017 年为世人所知。2020 年，改进的地面站光学系统使墨子号展示了另一个世界首创的技术——两个相距甚远的地面站之间基于纠缠的 QKD。与先前的工作相比，该研究将双光子分布的链路效率提高了约 4 倍，并获得了 0.12 比特/秒的有限密钥-秘密密钥速率。因此，该研究工作为基于纠缠的全球量子网络铺平了道路。



尽管时钟同步可能使人们难以理解，但其在网络运营，金融服务和导航等各种应用中扮演着重要角色。现有方法依赖于 GPS 、 GNSS 信号，但结果不太稳定，存在一定的误差。中国利用墨子号演示了利用量子信号（即单光子）作为载体进行所谓的时间传输。

与卫星进行量子通信并不容易，当前的方法仅限于夜间运行。这些因素将限制卫星 QKD 的商业可行性。中国正在努力解决这些问题，世界各地的一系列卫星项目也在争相追赶。

国家量子技术、太空计划以及日益发展的国际合作正在帮助加速推动该技术向前发展。

SpeQtre（前称 QKD Qubesat）是英国和新加坡之间的联合任务，将于 2021 年进入太空。它以 2020 年的 SpooQy-1 任务为基础，该任务成功成功地进行了光量子纠缠的演示实验。

QEYSSat 是由加拿大领导的任务，计划于 2022 年发射。最近的英国国家量子技术计划协议允许与其他国家进行卫星技术合作，并且使英国财团能够在 Craft Prospect 和滑铁卢大学的领导下为这项计划提供下行 QKD 链路系统 。

SAGA 是欧洲航天局计划中的任务，目的是演示两个地面站之间基于纠缠的 QKD，并且有望在现有的欧洲成果基础上发展。QUBE（德国）计划于 2020 年底发射，而 NanoBob（法国）计划于 2022 年发射。

英国 ROKS 是太空计划资助发现的一个阶段性成果，该成果可能在 2022 年进一步在轨演示 QKD 下行链路。其合作伙伴包括 Craft Prospect 和 Fraunhofer。

八、地面技术

地面技术也在迅速发展。2020 年的一个亮点是在多节点、远距离的量子网络中取得基础性突破。

英国 Bristol 大学的研究实现了 8 个节点的全互联网络结构，从网络层的角度看，任意两个节点之间都有纠缠关联关系。对于英国 Quantum Comms Hub 而言，这是一个了不起的成就。

量子技术旗舰项目 UNIQORN 还开发了 SDN 纠缠共享所需的 q- ROADM 技术。

另一个亮点是拓展了量子纠缠的光纤传输距离。2020 年，中国研究团队成功在两个由 50 公里光纤连接的量子存储器间实现量子纠缠，为构建基于量子中继的量子网络奠定了基础。尽管在世界各地的研究中均取得了不错的进展，它仍处于起步阶段。

欧洲 QIA 联盟的目标之一是利用不同的物理平台构建高效的纠缠存储设备，为量子中继器技术奠定基础。最近的突破是提高了量子存储器件的效率。

哈佛大学找到了一个新的方法，用于量子中继器的技术——金刚石 NV 色心。NV 色心是金刚石原子结构中的微小缺陷，可以吸收和辐射光，从而产生鲜艳的色彩。

Argonne Quantum Loop——美国能源部阿贡国家实验室在芝加哥郊区创建了一个 52 英里(83 公里）的“量子环路”， 目的是创建一个基于量子“纠缠”或亚原子粒子传输的并行、更安全的网络。该环路展示了通过产生并通过两个光纤环路传输光脉冲来测试平台的操作。

九、未来展望

实现真正的量子互联网仍有很长的路要走。但是，与当前互联网的出现类似，一开始的标准

和架构将会对未来产生长远的影响。现在了解量子互联网可能的应用领域可能有助于我们做出更好的决策。

盲量子计算——一种远程的量子计算模式，这有望简化从客户端发送所需的量子态。在量子时代，“盲”意味着量子服务商无法获得计算任务的全部信息，从而保证了计算的安全性。

一次性项目——UNIQORN 已完成一次性项目执行的原理证明。常规的互联网擅长传播内容，但不擅长保护 IP 地址。该量子协议开发了一套新的工具，在软件许可的情况下，可应用于一次性授权和电子投票系统。

手持式设备——英国的 Quantum Comms Hub 一直在致力于开发了便携式 QKD 设备。目的是通过创建用于 PIN 保护和身份验证的手持式消费者设备来增强现有应用程序的安全性，例如与 ATM 的交互。这是一项使量子互联网进入未来智能设备的技术，如非接触式支付、访问控制和数字签名。

Tim Spiller（Quantum Comms Hub 主任）总结道：“在较短的距离上，便携式 QKD 设备才能实现灵活性；在城市和城市之间可以利用光纤网络进行互联通信；对于远距离而言，量子卫星链接是一个不错的选择。未来的全球量子互联网则需要将这些技术结合起来。”

十、2021 展望

NIST 后量子密码标准化工作第 3 轮——预计将出现一个用于互联网和一般用途的 DS 和 KEM。两者都是基于结构化晶格的密码。预计 2022 年标准草案的制定过程将保持在正轨上。

NIST 后量子密码标准化工作第 4 轮——注意 NIST 额外一轮评估的更多细节。NIST 备选方案清单上的协议可能会出现。

QRNG 智能手机——这是否会超越利基用户的专业功能？如果它能向更广泛的受众证明这是一个低成本的附加组件和一个有吸引力的营销点，那么它可能是量子经济时代的第一个重大突破。

QRNG 市场——在更广阔的 QRNG 市场上，预计将在可用熵率（目前 QuintessanceLabs qStream 以 1Gbps 领先）、交换（KETS 有可用于其芯片级解决方案的开发板）和认证（CQC 指出其 Ironbridge 产品的自我验证特性）方面展开竞争。IDQ 在这一细分市场具有先发优势。客户需要知道 QRNG 设备能否做到其声称的功能。

QKD 玩家——东芝、SK 电信、英国电信、德国电信、西班牙电信、Orange 以及 Verizon 等大牌公司越来越积极地将这项技术商业化。注意商业渗透的最新进展。

CV QKD 系统现在也可以从 XT Quantech 和 QuintessanceLabs 获得，它们有自己独特的优点。关注这项技术的下一代：TF-QKD、MDI-QKD 和更先进的基于纠缠的方法。

中国的卫星 QKD——中国的下一个目标将是卫星对飞船的演示。关注 QKD 地面站的可部

署性。关注中国 QKD 卫星星座计划的细节。最初的设想是在 5 年内建立一个由 3-5 个 QKD 纳米卫星组成的网络，为 100 多个客户提供服务。

卫星 OKD 进展——QUBE（德国）将于 2020 年底发射。SpeQtre（前身为 QKD Qubesat，英国和新加坡）将于 2021 年推出。NanoBob（法国）预计将于 2022 年推出。QEYSSat（加拿大和英国）将于 2022 年发射。ROKS 资助了 2022 年 QKD 下行链路的潜在在轨测试。

欧空局 SAGA——关注欧空局计划的演示基于纠缠的 QKD 任务的新细节。

NASA——美国宇航局将宣布一个基于卫星的纠缠分发项目？

OpenQKD 测试平台——欧洲从马德里到日内瓦再到波兹南的 14 个中心正在为 QKD 现场试验和用户参与提供测试平台。

基于地面的纠缠——英国布里斯托尔打算在 100km x 30km 的区域内演示一个 19 节点的完全纠缠网络。这感觉像是工程学而不是物理学。

阿贡量子环路——将成为美国国家量子网络的起点。关注它对费米实验室的最初扩展，以及它在美国能源部 17 个国家实验室中的推广时间。

量子互联网模拟器——关注来自 QIA 和 Aliro Quantum 的工具，它们帮助我们模拟、理解并规划未来的量子网络。

量子区块链模拟器——初创公司 Quantum Blockchains 目标是创建下一代分布式账本技术。还有一段路要走，关注初始的模拟器产品，可以潜在的合作伙伴提供什么。量子技术可以为传统的区块链三重困境提供新的解决方案。

专利 EP 2537284——通过 CRNS，法国政府拥有一项广泛影响基于结构化晶格的 PQC 协议的专利。预计 NIST 和 CRNS 将达成协议，消除采用新 PQC 协议的任何经济障碍。

基于结构化晶格的加密——这一系列协议能够为当前的互联网安全提供“替代品”，但这些晶格中的附加“结构”允许它们具有相对较小的密钥尺寸，但这也是一个潜在的安全漏洞。

第七章：2021 量子计时、成像和传感展望

通用的基础技术正在开发越来越广泛的应用，以用于量子技术的各个领域。新产品在陆续上市，并且产品将层出不穷。创新型领导者正在为量子领域的研发者树立榜样，证明野心和收获是成正比的。量子的长期潜力巨大。

鉴于潜在的量子应用领域广阔，量子技术不仅涉及计算和网络，还在计时、传感和成像方面发挥着重要功能。研发的挑战通常是将技术带出实验室，并使它们可实际运用于现实生活中。

市场潜在的广度和复杂性使我们很难在面对研发的同时挖掘到相关的机会。我们应该关注些什么？

目标行业：医疗设备与诊断、航空航天与国防、汽车、资源、基础设施和土木工程；

形式：时间、重力、加速度、磁场或电场；

关键技术平台：冷原子、离子阱、金刚石、单光子、压缩光；

关键使能技术：光子学、微米/纳米制造、计算科学。

为了说明该行业目前的状况，Fact Based Insight 认为将重点放在市场上或相关的案例上。不过 2020 年的进展可以告诉我们未来量子领域发展的道路吗？

一、生物医学应用中的磁感应

当未来的历史学家写下第二次量子革命时，他们可能会提到基于约瑟夫逊效应超导量子干涉器件（SQUID），这是量子技术商业化的首次成功。这种设备中实质是一种将磁通转化为电压的磁通传感器。

1.OPMs（光泵磁力仪）

在用于非侵入性研究人脑活动的 MEG 扫描仪中，SQUID 技术得到了广泛的应用。基于 OPM-MEG 系统的 OPMs 使传感器不再笨重，可适用于所有群体。

经过四年的发展，初创公司 Cerca 已将 OPM-MEG 扫描仪用于临床评估，以便发现更多的临床诊断标志物和新的治疗机会。

这是一款基于 Quspin 传感器的 50 通道脑磁图记录仪阵列，该设备可保证传感器和每个测试者的头皮表面直接接触。被测试者戴上该头盔后，依然可以自由地进行头部活动。未来，测试者还可以穿戴该头盔进行社交活动等，不会受到任何影响，但该设计仍然需要在磁屏蔽室中使用。

MacQsimal 量子技术旗舰计划的一部分，致力于开发 OPM-MEG 扫描技术。

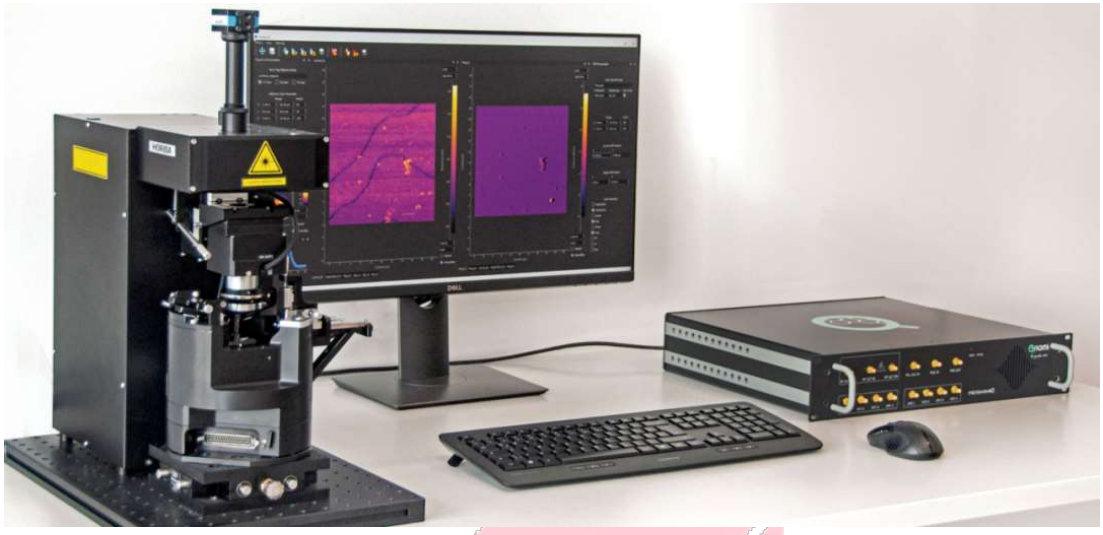
一些早期的量子初创公司已经研发 OPM 技术很多年。Cerca 面临的主要挑战包是如何保证头盔的“私人定制”性，使被测试者戴上该头盔后，依然可以自由地进行头部活动，同时保证收集到的数据的准确性。解决此类问题需要大量的技术人才和多样化的技能。国家量子技术计划不仅会为研发资金提供帮助，还会建立合适的网络。量子技术投资者需要选择合适的合作伙伴，并制定合理的研发计划。

MEG-BCI（脑磁图-脑机接口）可能是这项技术的更广泛应用。实验证明，带有 OPM-MEG 系统的头盔可作为人机界面使用。相反，目前的 ECG-BCI（脑电图-脑机接口）方法必须处理头皮的不良电学特性，或者需要进行侵入性手术以植入电极。

2. 金刚石 NV 色心

金刚石 NV 色心可以在环境温度下操作，虽然灵敏度不高，但是却可以实现小型化，并且其无毒性质使其特别适合现场生物测量。

近期，瑞士 Qnami 公司推出了一款量子扫描氮空位（NV）显微镜 ProteusQ。该系统一台磁场探测灵敏度是单原子层水平的磁性材料研究利器，能够以原子级扫描和表征磁性材料的样品。该设备易于使用，无需任何量子方面的专门知识，其合作伙伴 Horiba 现在正在推广该系统。



Qnami 受益于量子技术旗舰项目 ASTERIQS 的参与。该项目的合作伙伴还包括泰雷兹集团、博世、NVision 和比利时微电子研究中心，他们各自在金刚石技术上寻求不同的应用。这项技术有望带来许多令人惊讶的用途。

HP-MRI 是一种先进的核磁共振诊断技术，可以追踪注入人体的糖分并显示糖分变成什么。例如，在报告胸痛的患者中区分有生命/无生命的心脏组织时，这很有用。但是，由于生产该方法消耗的超极化分子缓慢且昂贵，因此该技术未被广泛采用。使用金刚石 NV 色心有望实现更快、成本效益更高且可部署的解决方案。

量子技术旗舰项目 MetaboliQs 正在寻求开发基于 NV 金刚石的 HP-MRI 技术。他们最近从概念验证转变为性能提高了 1000 倍的原型。

政府计划将在加速该技术适应各种应用方面发挥重要作用。另外对于分布式量子计算和量子互联网技术中的金刚石 NV 色心，投资者也不应感到惊讶。

二、2021 展望

路线图——英国宇航系统公司、英国电信公司和英国石油公司宣布了一个联合项目，为量子传感器商业化制定路线图。每一个都基于重要的量子技术经验。

美国 NQI——已经建立了三个中心，其中包括一个专注于量子传感的中心。预计美国将采取更多协调行动。

美国空军研究实验室——美国空军是量子计时和传感领域的重要参与者。关注他们的 AFWERX 和 Quantum Collider 项目。

计时技术——关注英国电信下一代计时的现场试验结果。关注 Teledyne e2v 的增强紧凑型原子钟。ColdQuanta 计划进入开发阶段。

磁力仪——关注 OPM 脑磁图的早期临床结果。关注增强大脑感知的新应用。

金刚石——金刚石 NV 传感器的目标是更广泛的生物医学应用。

重力仪——关注 Newton-g 正在埃特纳火山进行的实地研究结果。M Squared 重力仪的客户会出现吗?

太空中的冷原子——美国宇航局的冷原子实验室(建立在 ColdQuanta 的 Quantum Core 上)已经升级了原子干涉仪。关注卫星重力测量的原理证明。

导航——关注 M Squared 加速度计的第一批客户。ColdQuanta 计划从 2025 年开始其系统的开发阶段。

五眼联盟——澳大利亚、加拿大、新西兰、英国和美国正计划在 2022 年环太平洋演习中的一艘船上部署量子导航设备。我们会了解到更多吗?

射频感应——关注在高端无线设备测试中，太赫兹感应的应用不断增长。

量子雷达——关注入门级量子增强雷达的周边研究。预计时钟和频率稳定性将是关键主题。

关于光子盒

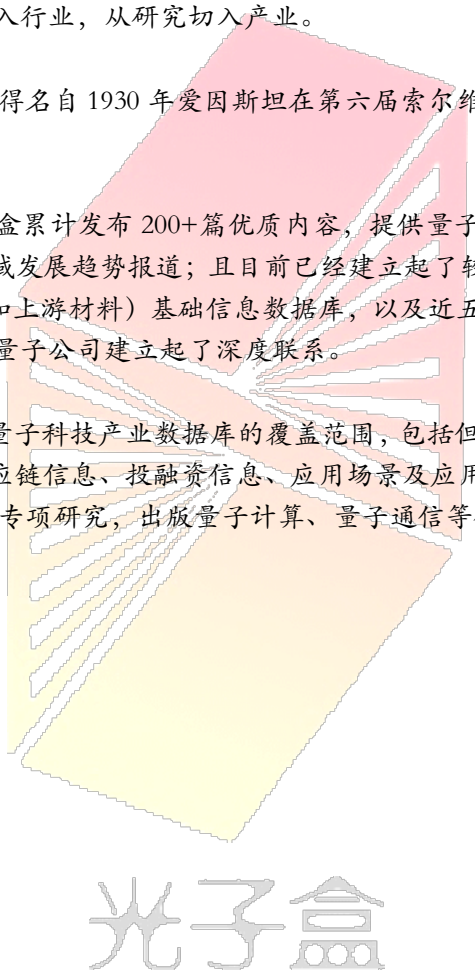
北京鹞鸟科技有限公司旗下的“光子盒”致力于成为一个中国量子科技产业基石服务商。以赋能量子科技产业参与者更高的成就为使命，链接企业、专业人才、投资者、个人用户等社群，加速信息、人才、资金、技术等要素的充分流动，推进中国量子科技产业快速、稳定向前发展。

目前量子科技产业化首当其冲的难题是，市场不了解这个行业，所以我们最先要成为量子科技传播者，从媒体开始切入行业，从研究切入产业。

光子盒始于 2020 年 2 月，得名自 1930 年爱因斯坦在第六届索尔维会议上提出的著名思想实验。

在近一年的时间里，光子盒累计发布 200+篇优质内容，提供量子科技前沿资讯、量子科技类企业报道、量子科技领域发展趋势报道；且目前已经建立起了较为完善的全球量子（包括通信、计算、测量、软件和上游材料）基础信息数据库，以及近五年全球量子产业投融资信息数据库，并与国内主要量子公司建立起了深度联系。

未来，我们还将继续扩大量子科技产业数据库的覆盖范围，包括但不限于：企业、技术人才、产品线、产业链图谱、供应链信息、投融资信息、应用场景及应用案例等，建立多维度的量子产业数据信息;以及开展专项研究，出版量子计算、量子通信等领域的年度白皮书。



公众号：光子盒
邮箱：caixq@chinaquantum.com
地址：北京市东城区朝阳门SOHO1506