

量子技术全景展望（2022）

量子硬件、算法、软件、互联网

Quantum Outlook 2022
Quantum Hardware, Algorithm, Software, Internet

2022 年 7 月

编者序

本报告原作为 Fact Based Insight 在 2022 年初发布的 2022 年《量子硬件展望》、《量子算法展望》、《量子软件展望》、《量子互联网展望》四篇文章，光子盒对其进行了编译并形成这份报告。

通过这份报告，并结合光子盒的报道，读者可以细心观察这半年时间量子信息科技领域的进展，对比报告中的预测，哪些是已经实现的，哪些是即将实现的？

目录

第一章 量子硬件展望	1
一、超导量子比特迎风而上	2
1、IBM 在基础路线图取得重要进展	2
2、谷歌蓄势待发，准备下一次飞跃	5
3、中国科学技术大学祖冲之掀起热议	7
4、Rigetti 专注于模块化	9
5、D-Wave 加速前进	10
6、众多参与者推动技术发展	11
二、离子阱：通往逻辑量子比特	12
1、IonQ 大放异彩	12
2、AQT 展示了一个真正的基于机架的系统	15
3、霍尼韦尔成立 Quantinuum，并继续交付产品	16
4、离子阱互连的创新	17
5、离子阱门的创新	17
三、光子学揭示了它的另类前景	18
1、PsiQuantum 迈出重要一步	18
2、中国科学技术大学九章 2.0 继续前进	22
3、Xanadu 详细介绍了自己的路线	23
4、QuiX 继续销售处理器	25
四、中性原子引领量子模拟	25
五、硅自旋量子比特实现三次飞跃	27
六、NV 色心有其独特的潜力	30
六、猫量子比特开始成形	31
七、正确的事情	31

八、展望 2022	32
第二章 量子算法展望	34
一、我们实现了什么?	35
二、寻找广泛的量子优势	37
1、变分量子算法	37
2、用于组合优化的量子退火	41
3、量子加速蒙特卡洛技术	43
4、量子机器学习	44
三、早期容错机器	48
1、平方加速还不够?	48
2、AlphaFold 与蛋白质折叠	49
3、哈密顿量模拟和 FeMoco	51
四、长远眼光	53
1、量子算法的大统一理论	53
2、BQP (有界错误量子多项式时间) 可轻松解决?	54
五、展望 2022	56
第三章 量子软件展望	58
一、量子先驱	59
二、早期门模型量子计算全栈公司	61
三、量子平台即服务	63
四、量子模拟器	65
五、量子软件初创公司	66
1、寻求长期支持	66
2、从算法到应用	67
3、更好的量子工具	71
六、建立低层控制	74

七、量子教育	77
八、当前的研究主题——房间里的大象	78
九、展望 2022	80
第四章 量子互联网展望	82
一、直接威胁	82
二、后量子密码到达拐点	83
1、问题类别的多样性很重要	86
2、迁移是一个更大的挑战	87
三、量子密码提供了一个不断发展的工具集	88
1、量子随机性很重要	89
2、带外密钥传递	91
3、量子密钥分发 (QKD) 基本成熟	93
4、标准在成倍增加	98
5、数学与物理之间的紧张局势持续发酵	99
四、太空带来了新的潜力	99
1、卫星 QKD 火起来了	100
2、纠缠分发的敲门砖?	102
五、未来的量子网络即将出现	102
1、量子网络指数级地增加量子计算机的能力	102
2、高级密码协议的持续进展	103
3、联网量子传感器的突破?	104
4、实验室中的纠缠网络	105
六、策略之争	107
七、展望 2022	107
声明	110

关于我们	111
------------	-----

图目录

图 1 IBM 127 量子比特处理器 Eagle	3
图 2 谷歌量子计算路线图	7
图 3 祖冲之二号 66 比特量子处理器	8
图 4 D-Wave Advantage	10
图 5 IonQ 量子计算机	13
图 6 AQT 机架式量子计算机	15
图 7 霍尼韦尔 H 系列量子计算机的量子体积	16
图 8 PsiQuantum 量子计算芯片	19
图 9 中国科学技术大学九章二号	22
图 10 Xanadu 可编程光量子计算机 Borealis	24
图 11 QuEra 256 比特量子模拟器	26
图 12 由 10 个量子点链组成的原子级量子集成电路	29
图 13 量子随机数平台 Quantum Origin	36
图 14 变分量子算法示意图	37
图 15 量子退火用于组合优化	42
图 16 阿里巴巴股价的蒙特卡罗模拟	44
图 17 蛋白质折叠	51
图 18 量子堆栈	58
图 19 领先的量子公司	61
图 20 早期门模型全栈公司	62
图 21 量子 PaaS	63
图 22 量子模拟器	65

图 23 算法到应用	69
图 24 量子工具	74
图 25 建立低层控制	77
图 26 当前研究主题	79
图 27 迁移至后量子密码	88
图 28 欧洲量子通信基础设施计划	96
图 29 中国“墨子号”量子卫星	100

表目录

表 1 不同加密技术的对比	83
表 2 高级密码协议	103

第一章 量子硬件展望

巨额投资创造了越来越多的量子独角兽企业。中国在光子和超导量子比特方面的进步引起世界关注。离子阱因逻辑量子比特的演示而大放异彩。但是谁能在建造实用量子计算机的竞赛中获胜呢？

我们应该从哪里开始评估最重要的量子硬件发展？不同量子比特平台面临的挑战和机遇差异显著。我们越来越需要了解每家公司优先考虑的目标，以及它们之间的相互关系。参与者是否都能顺利地实现自己的量子路线图？

容错量子计算机（FTQC）——早期容错量子计算机的新兴标准是一种具有 100 万物理量子比特的设备，运行表面码（或类似）纠错，以提供多达 1000 个逻辑量子比特。为了实现这一点，假设双量子比特（2Q）门保真度达到 99.9% 以上，并且量子比特相干寿命足够长，以至于它们不会支配错误预算。为了实现这一目标，公司需要证明他们可以从根本上扩大技术规模。具体的挑战因量子比特平台而异，但看起来并不容易：制造公差、过度的控制布线/激光对准复杂性、串扰/校准、热负载和冷却性能、量子互连以及用于控制和纠错的经典处理的延迟。在大多数方法中，创建“魔法态”（magic state）（支持通用门集所需的资源）看起来像是一个关键瓶颈。

含噪声中等规模量子（NISQ）——一些参与者强调使用更适度、嘈杂、中等规模的量子设备可能会更快实现。这避免了量子纠错所需的巨大开销，而是寻求在少量步骤（浅电路深度）完中成计算，以便每个物理量子比特引入的错误不会变得难以处理。认为，门模型量子计算机要在实际应用中获得广泛的量子优势，可能需要 99.99%+ 的 2Q 保真度。增强的甚至是针对特定问题的量子比特连接也可能非常重要。将需要与经典处理进行低延迟集成。

较少量子比特的量子计算机（FQCC）——同样重要的是要记住，对于某些应用，我们只需要“几个量子比特”。此类应用的早期示例通常位于量子计算、网络安全和量子通信的交叉点；这种重叠有望最终发展成为量子互联网，并通过传

感器发展成为量子物联网。这里的不同权衡最终可能适合不同的量子比特平台。能够在更高、更容易部署的温度下提供一些相干寿命可能是一个有用的优势。

扩大规模是很困难，但对于许多硬件公司来说，这是一件好事，他们可以指出他们的多量子比特设备从上一代到下一代都在提高保真度。然而，几乎在所有情况下，他们仍在“追赶”理想的双量子比特（2Q）实验室设备所能实现的目标。坦率地说，我们今天看到的保真度根本不够好。

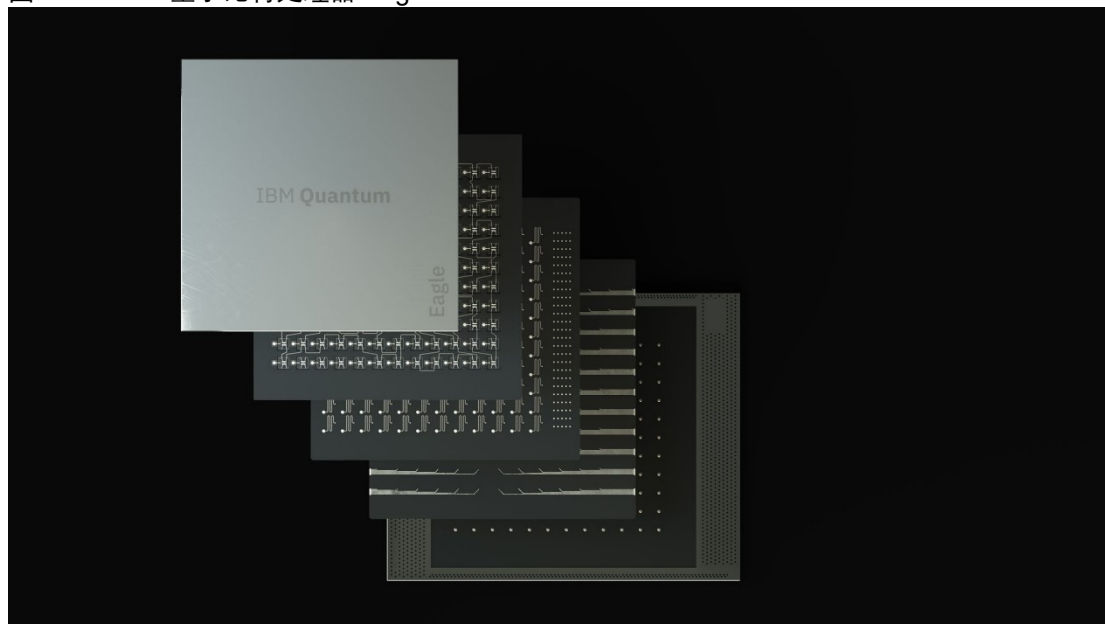
多年来，门模型量子计算平台的非正式入门级基准一直是证明 2Q 门保真度高于 99%。随着经验和实际关注的增加，这个领域现在需要认识到最低指标是 99.9%（或者你需要提供一份来自量子纠错负责人的非常明确的说明，说明为什么这个标准不适用于你）。正如我们将看到的，在 2021 年，公司已经同时采用这两种方法。

一、超导量子比特迎风而上

1、IBM 在基础路线图取得重要进展

2021 年，IBM 推出了迄今为止最大的处理器——127Q 的 Eagle。我们还不知道这款处理器将提供什么样的量子体积（QV），尽管至少在短期内这肯定会受到保真度而不是量子比特数的限制。但是 Eagle 已经令人印象深刻。IBM 团队显然非常兴奋，因为他们成功地制造出了一种新的多层芯片架构，其中包括量子比特、读出谐振器和不同层上的控制线。这大大简化了控制路由的挑战，并证明了进一步扩展的概念。重要的是，IBM 还在继续证明他们有能力将前几代处理器的性能提升到超越早期极限的水平。

图 1 IBM 127 量子比特处理器 Eagle



我们认为，IBM 最近在基础保真度统计方面取得的进展尤为重要。Falcon 系列设备现已取得一系列令人鼓舞的成果：

R8 修订版现在稳定实现约 0.3 毫秒 (T_1) 的平均寿命。测试设备已达到 0.6 毫秒。长寿命最终是整体保真度的重要基础。当量子比特必须等待其他操作完成时（例如在纠错周期中），它们也很重要。长寿命的状态一直是 IBM 固定频率 transmon 量子比特的承诺，因此其他参与者不一定容易匹配。

在 2021 年的一项引人注目的公告中，Falcon R10 上最好的 CNOT 门现在达到了 99.91% 的 2Q 门保真度。以前 IBM 处理器系列的趋势令人印象深刻。此外，IBM 还发布了带有实验设备的有希望的结果，探索了架构的变体，例如可调谐耦合器的引入。小型测试设备报告了令人鼓舞的结果，其 2Q 保真度为 99.85%。该技术还应有助于抑制同时操作中的串扰。

IBM 的进展很重要，因为它让我们有理由相信，使用当前的材料和制造技术在大型设备上达到 99.9% 的 2Q 保真度仍然是一个合理的预测。如果我们不得不依赖材料科学的进步或全新的制造技术，那么该行业目前激进的时间表只会令人失望。

IBM 在其约克镇高地的 200 毫米试验生产线上制造自己的芯片。它指出在超导量子比特的特定背景下，这是最先进的技术。这似乎使它有信心继续制造具有越来越多量子比特的单个芯片。IBM 还提到了其广泛的专利组合，以及在保护其制造技术方面可以发挥的作用。

IBM 还为早期量子设备引入了一种新的性能指标。以前的测量方法都试图捕获设备大小（量子比特数）或质量（QV），而新的测量方法（CLOPS）则聚焦于速度——一个（有争议的）具有代表性的操作样本能够以多快的速度完成。

量子比特数——可用量子比特的数量（相互连接，可用于 2Q 门）仍然是一个关键指标。因为在 50Q 以下，我们仍然可以模拟量子计算机用传统计算机能做的大多数事情。

量子体积——该指标衡量设备可以执行的最大随机“方形”电路。这将量子比特宽度与 QV 层中的电路深度相结合。每层都是量子比特的随机排列，然后是所有对之间的随机 2Q 门（特别是 SU(4) 门）。所需的物理电路深度通常远大于 QV 层的数量，因此该指标不仅体现了量子比特门的保真度，还体现了灵活的原生门组、增强的量子比特连接、有效的编译器路由和低层错误缓解带来的好处。

每秒电路层操作数——该指标衡量处理器每秒可以执行的 QV 层数（平均超过 100 次运行）。这保持了一种与硬件无关的方法，使我们不仅可以衡量快速门的影响，还可以衡量高保真快速读出、低延迟控制系统和低级编译器性能的影响。

量子计算支持者过去倾向于忽视原始处理器速度，而是依赖于这样一个假设，即执行的算法中的优势总是会使拥有最大量子能力的量子计算机获胜。然而，越来越深入地了解真实机器所面临的挑战，迫使我们更加具体地看待问题。在短期内，需要在 NISQ 设备上的合理时间范围内执行高重复变分算法。此外，当前的 FTQC 架构看起来太慢，无法为仅提供平方加速的算法提供优势。更快的量子门会有所帮助。

任何基准是否有用的一个关键测试是，它是否有助于该领域专注于需要解决的实际问题，还是只是参与指标衡量？我们认为，量子比特数、QV 和 CLOPS

加在一起，可能被证明是 useful 的高级指标。2019 年，IBM 设备仅提供 16 QV 和 200 CLOPS（推断）；现在他们在一系列可访问云的 Falcon 处理器中提供 128 QV 和 2000+ CLOPS。

Eagle 是最后一款使用 IBM Quantum System One 机箱的处理器。IBM 宣布 IBM Quantum System Two 作为未来芯片的外壳。它采用模块化六边形概念，包括控制电子设备和低温技术。提供足够的冷却能力和最小化停机时间是超导量子比特的另一个扩展挑战。IBM 引入了专业合作伙伴 Bluefors 来帮助解决这一问题。冷却能力的提升也为未来使用量子互连的处理器之间的相干网络打开了大门。

IBM 路线图——127Q（Eagle）2021、433Q（Osprey）2022、1121Q（Condor）2023；100 万 Q 的大规模系统。通过重六边形码（混合表面码和 Bacon Shor 码）进行纠错。首选指标：量子比特数、QV 和 CLOPS。

OQC 是一家英国超导量子比特初创公司。与大多数其他超导量子比特竞争对手相比，OQC 也一直在使用固定频率的量子比特。公司的专利 coaxmon 量子比特架构是根据基本原则设计的，以缓解 IBM 在 Eagle 中使用堆叠方法解决的相同路由问题。看看数据对比会很有趣。

OQC 是第一家通过亚马逊支架云平台提供处理器的非北美公司，这是一个值得注意的里程碑。此外，该公司还推出了英国首个商用 QCaaS 服务。

2、谷歌蓄势待发，准备下一次飞跃

谷歌计划到 2029 年斥资“数十亿”美元开发 QC，并将其团队规模扩大一倍。它现在还拥有自己的洁净室，可以缩短制造芯片的周期。

谷歌率先实现了其第一个里程碑：他们的 Sycamore（悬铃木）芯片展示了超越任何经典计算机的计算能力（量子优越性）。他们现在正按计划实现第二个里程碑：逻辑量子比特原型。他们想证明他们首选的纠错方法，即表面码，确实可以通过增加网格大小来系统地抑制错误。

为了实现这一目标，他们实施了升级，将悬铃木架构从一种专门针对“随机

电路采样”的人工问题转向为实现表面码而优化的架构。这包括将他们本机实现的主要 2Q 门升级为对手头任务更有用的门。

类 iSWAP→CZ——与可调谐频率转换量子比特保持一致，新标准 CZ 门比旧门更复杂且速度稍慢（14ns → 26ns）。这是一个真正的成就，它具有大致相同的保真度（99.4% 2Qsim——还需要注意的是，谷歌引用了同步操作中更严格的 2Q 保真度测试，其最好的单个门对之前已经证明了 99.9% 的性能。

读出和复位——谷歌还实现了更快和更高保真度的读取，从 3000ns 和 96.2% 提高到 600ns 和 98.1%。一种新的多级复位操作也能够纠正泄漏错误。

谷歌在读取性能方面的改进对于纠错至关重要，因为闲置数据量子比特上的错误已被证明是一个令人惊讶的重大瓶颈。2021 年，谷歌已经成功实现了一个一维“重复码”，可以看作是完整二维表面码进程的中途标志。

Lambda (Λ) ——谷歌强调了参数的重要性，该参数用于衡量当我们移动到更大的代码距离时如何有效地抑制错误。 Λ 大于 1 表明系统纠错正在起作用，但谷歌认为 Λ 为 10 是系统设计的最佳点。低于这个值，物理量子比特与逻辑量子比特的比率会不切实际地增加，高于这个值会提供相对递减的回报。因此，为了实现这一点，目前的表面码协议被认为需要 99.9%+ 的 2Q 门保真度。在测量和重置周期期间等待的闲置量子比特的错误率也必须显著提高。

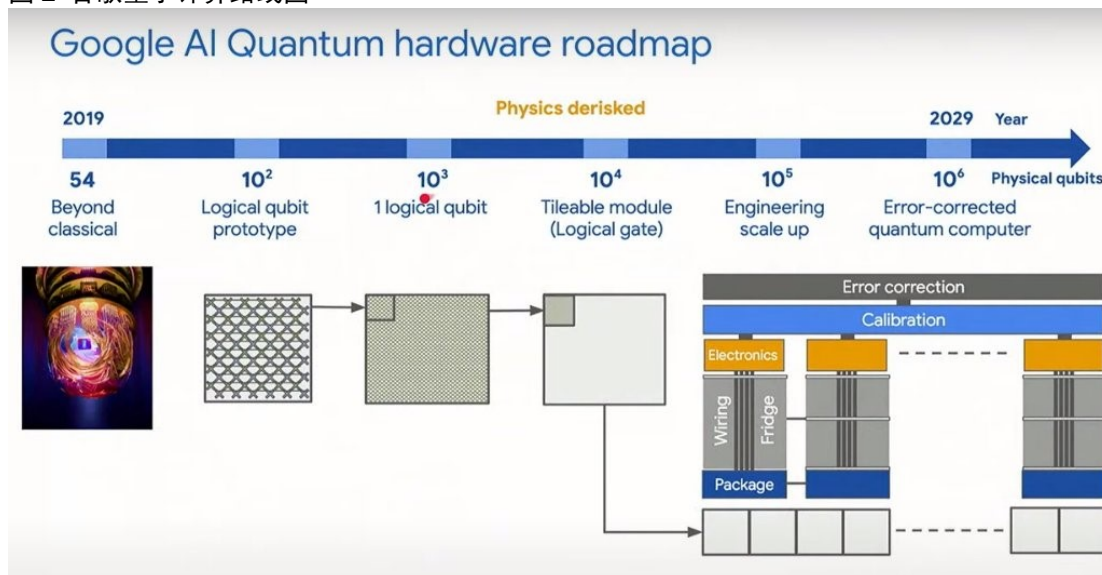
错误突发——并非所有错误都是一样的。纠错码通常被设计为在错误很小且无关的假设下工作。量子比特状态被破坏的泄漏错误，或跨多个量子比特高度相关的错误更难以管理。谷歌指出，减轻宇宙射线和潜在放射性的影响，现在是进一步扩展的现实设计考虑因素。

Hartmut Neven 指出：“在《自然》杂志上写一篇论文，超越经典能力是一回事，让它随着时间的推移而可靠地运行，并提供合适的云服务水平，则是另一回事。”这并不是消极的，而是一个例子，说明随着设备规模的扩大，自动化校准等实际挑战是多么艰巨。这是其他人可能很快面临类似问题的一个标志。

谷歌路线图——从现在到 2029 年，逐步实现 100Q（逻辑量子比特原型）、

1000Q（逻辑量子比特）、10000Q（可平铺逻辑模块）、10 万 Q（工程放大）、100 万 Q（纠错量子计算机）。通过表面码协议纠错。首选指标：同时操作中的 2Q 门保真度。

图 2 谷歌量子计算路线图



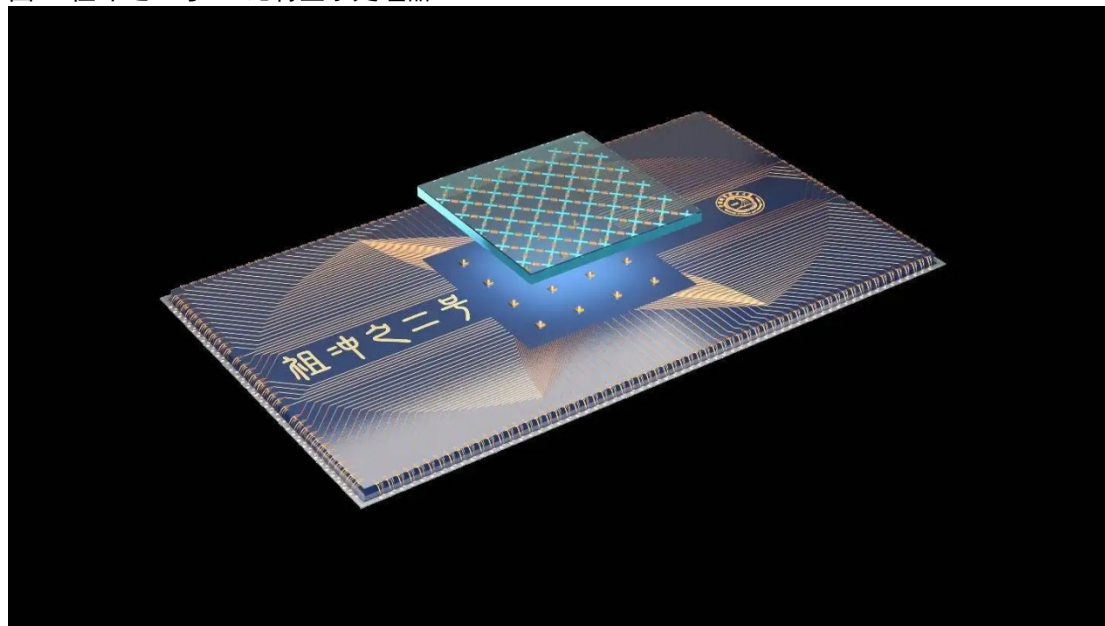
QuTech 也研究可调谐频率 transmon 量子比特，并发布了令人震惊的保真度结果。在实验室测试设备中，QuTech 研究人员实现了保真度为 99.93% 的新型 SNZ CZ 2Q 门。这对 Quantum Inspire 开放接入云的未来是一个好兆头。此外，MIT 还展示了一个高保真度的 iSWAP 2Q 门，带有保真度为 99.87% 的可调谐耦合器。

该类型的系统面临的校准问题反映在 UKRI（英国研究与创新中心）在这个领域资助的工作中。由初创公司 Riverlane 领导的 AutoQT 项目正在寻求利用人工智能技术来保持量子比特旋转。

3、中国科学技术大学祖冲之掀起热议

2021 年，中国科学技术大学凭借 66Q 超导量子比特器件“祖冲之”登上头条。祖冲之 2.0 能够执行 56Q 的随机电路采样，祖冲之 2.1 能够执行 60Q，比悬铃木多 7 个量子比特，实现了一项新的计算难度世界纪录。

图3 祖冲之二号 66 比特量子处理器



祖冲之——以中国天文学家和数学家的名字命名，他在公元 480 年左右精确计算出圆周率的数值，此后 800 年无人超越。该设备采用与谷歌悬铃木基本相同的架构：可调谐频率 transmon 量子比特，并带有可调耦合器以抑制串扰，以及类 iSWAP 门。

这是否意味着中国科学技术大学目前在 QC 竞赛中处于领先地位？祖冲之的保真度统计数据（99.4% 2Qsim）现在与“悬铃木”不相上下，尽管它的门速度比最初版本的“悬铃木”要慢（24ns vs 12ns）。用科学术语来说，这是在另一个实验室重复实验以确认结果的一个很好的例子。中国科大研究团队现在面临着 Google 在过去两年中一直在寻找的相同挑战；如何将一个伟大的实验变成一个足以正常运行的设备。读出保真度在祖冲之 2.0 版和 2.1 版之间提高的速度令人振奋，制造新的芯片只需要 2 个月的时间，这也许是我们可以期待的指标。更具挑战性的是如何在量子比特保真度上领先，而不是追赶。中国科大和 Google 的保真度都不足以达到他们想要实现的目标。

随着中国超导量子比特技术的发展，总部位于合肥的量子计算初创公司本源量子（Origin Quantum）处于有利地位。它已经支持 24Q 系统的云访问，并即将

升级到 64Q。在一轮成功的融资后，本源量子的估值达到 70 亿元，成为独角兽。

本源量子路线图——2021 年 64Q、2022 年 144Q、2025 年 1024Q。

中国的超导量子比特技术有望受益于在山东济南正在建设的新一代最先进的下一代纳米制造中心。这将是竞争日益激烈的比赛的关键帮助。

在欧洲，量子旗舰（Quantum Flagship）项目 OpenSuperQ 已经构建了初始的 5Q 和 7Q 超导量子比特设备，也采用了可调谐量子比特方法。目前工作计划结束之前（2022 年 3 月之前），有可能升级到 20Q 倒装芯片设计。这将低于该项目最初的 100Q 目标。然而，认为，我们必须现实地看待这类前沿项目是否能够持续追赶承诺的时间表。如果他们总是能做到，那我们的野心就太低了。同样，面临的困难也突显了中国科大团队在开发祖冲之方面取得的成就。

在保真度这一关键指标方面，阿里巴巴也取得了重要进展。今年 3 月，阿里巴巴达摩院量子实验室成功设计制造出两比特超导 fluxonium 量子芯片，实现了两比特 iSWAP 门保真度最高达 99.72%，达到了超导量子比特全球最佳水平。

4、Rigetti 专注于模块化

2021 年，Rigetti 已经取得了令人振奋的成绩。去年 10 月，Rigetti 宣布以 SPAC 为基础的上市交易成为头条新闻，这使得他们也成为量子独角兽企业。

制造规模不断扩大的单个芯片面临着量子比特失效和产量下降的问题。Rigetti 强调了模块化方法的发展，该方法直接针对这种扩展性挑战。在独立的硅模具上制造的小型处理器被倒装到载体芯片上。该载体芯片采用耦合器，以提供独立芯片之间的量子相干互连。这种方法能保持所需的高保真度吗？2021 年的结果显示出了希望。跨芯片纠缠率可与 Rigetti 的基本门速度（约 10 MHz）相媲美；保真度是有希望的（iSWAP 为 99.1%，CZ 为 98.3%）。

最后，许多公司可能希望使用这种方法。但最佳制造芯片尺寸的交叉点仍然有待确定。显著提高保真度是 Rigetti 面临的重要挑战。

5、D-Wave 加速前进

D-Wave 在 2021 年对其战略进行了非常重大的扩展,宣布计划推出基于门的系列设备。他们计划的细节非常有趣。他们承认,量子计算的门模型方法对材料科学和化学模拟问题具有更大的长期潜力(使其符合该领域的传统智慧)。然而,他们也很清楚,他们在量子退火上下了双倍的赌注,因为他们认为该架构在短期和长期(至少与目前设想的门模型架构相比)都有最佳的优化问题前景。

D-Wave 退火路线图——5000Q Advantage 15 路连接, Advantage 性能更新 2022 年; Advantage 2 新的量子比特设计 2023/24 年,改进的相干性实现了改进的连接性 2025 年。

图 4 D-Wave Advantage



D-Wave 门模型概念也很独特,保留了他们开创的通量量子比特设计和多层制造,包括在芯片上保持多路复用控制。许多人认为这些折衷方案不适合门模型方法所要求的高保真度规格。不过, D-Wave 有相关专家。如果他们不相信自己能成功,他们就不必定义这条道路。

D-Wave 门模型路线图——第 1 阶段验证多层堆栈中的量子比特;第 2 阶段验证纠错;第 3 阶段演示逻辑量子比特操作;第 4 阶段:设计可扩展的特定任务

组件；第 5 阶段：第一个集成通用处理器。

Qilimanjaro 是一家西班牙初创公司，也在追求量子退火技术。它正在参与 AVaQus 项目，在欧洲建造一个相干量子退火器。

6、众多参与者推动技术发展

SEEQC 基于其独特的超导单通量量子（SFQ）数字控制技术成为该细分市场具有长期潜力的另一家初创公司。

单通量量子——这种独特的超导电子技术使 SEEQC 能够在单个低温芯片上集成快速、低热量和低功耗的经典处理、数字多路复用和低延迟量子比特控制。基于 SFQ 电路的快速经典控制逻辑，尤其是纠错和魔法态的有效生成，可能是 SEEQC 的一个关键优势。

高效的倒装芯片——SEEQC 方法的一个优势是超导量子比特和超导控制电子设备的相对尺寸相似：量子比特位于一个晶片/芯片上，而相应的 SFQ 控制电路位于另一个相同尺寸的晶片/芯片上。这些可以使用已建立的晶圆厂工艺单独制造、切割和倒装芯片键合。这种制造灵活性与无线耦合相结合，有望带来扩展优势。

SEEQC 最近制造了他们的第三代多芯片模块测试设备，包括与 SFQ 控制器相结合的 transmon 阵列和 fluxonium 设备，但尚未对性能统计数据发表评论。

SEEQC 的集成量子比特控制方法吸引了众多投资，并在 2021 年获得了英国 UKRI 的三笔拨款。SEEQC 拥有最先进的内部商业晶圆厂，能够生产复杂的 SFQ 芯片，这意味着他们将从美国支持芯片制造技术投资的政治势头中受益。

IQM 是一家提供差异化服务的欧洲初创公司，专注于为研究机构和高性能计算（HPC）中心构建现场量子计算机。这种协同设计方法有很大的优势，特别是在欧盟和印度等具有潜在独立意识的亚洲国家。2021 年 IQM 中标了一个备受瞩目的项目，该项目将在德国构建量子计算系统。

Bleximo 是一家美国初创公司，也专注于基于超导量子比特的特定应用量子

计算机的协同设计。尽管迄今为止他们一直保持低调，但他们的工程能力在 Q2B 会议上得到了清晰的展示。Bleximo 自然受益于其与加州大学伯克利分校的密切联系。

IMPAQT 是一个荷兰财团，其目标是研究团队的“自建”市场。

未来超导量子计算机的可扩展性也将在某个时候可能需要独立稀释制冷机之间的相干连接。苏黎世联邦理工学院已经证明了这一原则。量子旗舰 QMiCS 项目引领了这项技术在欧洲的发展。

二、离子阱：通往逻辑量子比特

1、IonQ 大放异彩

离子阱在 2021 年占据了许多头条新闻。IonQ 以其吸引眼球的 20 亿美元的 SPAC 上市敲响了纽约证券交易所的钟声。

IonQ 的学术合作者还更进一步，演示了 15Q 设备的容错控制，以形成单个逻辑量子比特（使用 Bacon-Shor-13 纠错码）。演示了一套完整的单量子比特门，以及魔法态的创建。这是容错领域的一个里程碑，尽管所实现的逻辑保真度仅为中等（逻辑 SPAM 保真度为 99.4%，逻辑 1Q 保真度为 99.7%）。由于纠错经常被讨论，以至于有些人可能认为这是理所当然的。看到它在实践中发挥作用，这个领域应该松了一口气。

IonQ 也取得了独立基准测试的成功。2021 年，美国量子经济发展联盟 QED-C 发布了一套涵盖一系列通用基础量子算法的性能基准。结果包括 IonQ 的云访问 11Q 系统和 IonQ 的下一代硬件。与上一代相比，最新的 IonQ 硬件迈出了一大步，在测试中总体上优于 IBM、霍尼韦尔和 Rigetti 的其他设备。由 QED-C 开发的信息可视化使得离子阱系统提供的增强量子比特连通性的好处得到了清晰的演示。

QED-C 基准套件——它选择了广泛讨论的量子算法，并展示了它们在不同量子比特数量和电路深度上的性能。生成的可视化效果很好，信息量很大。它们

支持与 QV 的直观联系，并提供超越简单数字的洞察力。

该系统的测量 QV 尚未公布，但据估计，在基准测试时，该系统的 QV 似乎在 1024QV 范围内运行，仍远低于我们希望看到的 400 万 QV。IonQ 似乎在调整 2Q 门保真度以充分发挥系统潜力方面面临延迟。

IonQ 路线图——2021 年 22AQ、2023 年 29AQ、2025 年 64AQ、2026 年 256AQ、2027 年 384AQ、2028 年 1024AQ。纠错开销——2025 年 16:1，2027 年 32:1。

算法量子比特（AQ）——IonQ 定义的指标，表示可用于计算的“有效完美”量子比特的数量（请注意，可用的逻辑门深度仍然有限）。在没有纠错的情况下， $AQ = \log_2(QV)$ 。

图 5 IonQ 量子计算机



IonQ 策略的一个关键部分是采用灵活的纠错方法。与其等待实施高性能高开销表面码，不如强调中期计划以务实地使用较小的码。这有望以适度的开销（16:1）提高保真度（可能达到 99.99%）。

超导挑战——IBM 的 $99.91 \pm 0.014\%$ 、QuTech 的 $99.93 \pm 0.24\%$ 和 MIT 的 $99.87 \pm 0.23\%$ 的超导量子比特的 2Q 门保真度是对离子阱的一个重大挑战。离子阱

系统的一个关键优势是它们提供了更高的 2Q 门保真度。然而，激光驱动门只有 $99.92 \pm 0.04\%$ ，近场微波驱动门为 $99.91 \pm 0.09\%$ ；而这些水平的表现只在简单的 2Q 实验室实验中得到了证明。没有一个离子阱团队在真正的多量子比特设备中展示过类似的东西。IBM 实现了与离子阱系统不相上下的保真度，并且是生产制造系统。超导量子比特门的速度也明显更快。

离子阱系统还有更多的路要走。增强的量子比特连通性可能与潜在的 NISQ 应用非常相关（超导量子比特通常限制在最近邻的相互作用）。如果它允许以降低的开销获得创新的纠错码实现，可以转化为重要的长期利益。在超导量子比特门保真度的可变性中，我们还可以看到另一个经常被强调的问题的直接证据：制造的量子比特具有不可避免的可变性，而基于离子或原子的量子比特不会。

在 2021 年 Q2B 大会上，IonQ 宣布了其技术路线图的新细节。它的下一代处理器将使用钡离子量子比特，而不是当前设备中的镱离子。并不期望在性能上立即出现飞跃，但总的来说，这很好地说明了 IonQ 技术愿景的蓝图。拥有 8 亿美元投资基金的一个微妙挑战是，你是否有足够的好主意来让这些钱发挥作用。IonQ 在商业和科学方面的领导地位似乎正在抓住这个机会。

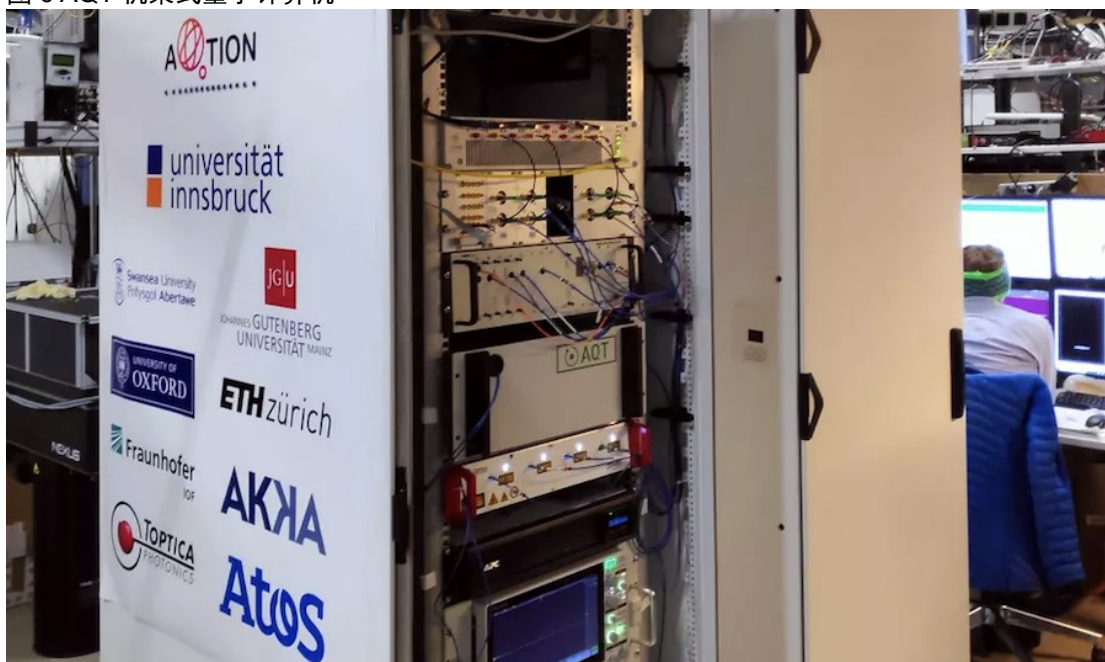
钡离子量子比特——钡-133 不是自然产生的。这种人造同位素是专门合成的，因为它有望成为俘获离子量子比特。它的核自旋为 $\frac{1}{2}$ ，因此可用作长寿命超精细量子比特的基础。至关重要的是，离子的电子结构也具有在方便的光波长处跃迁的亚稳态。这些在光纤或集成光子设备中更容易使用。这种转变可用于更方便地操纵超精细量子比特，或作为在同一系统中形成光学量子比特的基础。这也有望简化在陷阱之间创建光子互连的任务。与其他离子种类相比，钡离子的实验工作仍处于相对早期的阶段。

IonQ 非常强调他们方法的模块化。该公司首席科学家 Chris Monroe 指出，即使在转移到多个设备之前，离子链也可以在单个扩展陷阱中移动和组合，以创建数百个量子比特的模块。集成光学是扩展的关键要求，但他指出这是一项工程挑战，而不是物理挑战。

2、AQT 展示了一个真正的基于机架的系统

奥地利的阿尔卑斯量子技术公司（AQT）是一家基于捕获离子光学量子比特（基于光学跃迁，而不是 IonQ 和霍尼韦尔使用的超精细跃迁）的初创公司。虽然相干时间稍短，但承诺更容易集成光学系统的未来发展。AQT 利用他们在欧盟 QT 旗舰 AQTION 项目中的参与，交付了第一个 24Q 全机架式演示系统，这是当今世界上最小的 QC 系统。

图 6 AQT 机架式量子计算机



在 2021 年 EQTC 会议上，AQTION 和因斯布鲁克大学团队展示了一套完整的通用容错门（1Q 门、2Q 门和魔法态注入）。这个世界上第一个使用 16Q AQT Pine Trap 设备来实现 2 个逻辑量子比特（每个使用 7Q 色码，也称为 Steane 码）。Thomas Monz 领导着因斯布鲁克团队，同时也是 AQT 的联合创始人。如果这一结果能够通过同行评议，那将是欧洲计划的重大胜利。

Pine Trap 的 2Q 保真度为 99.36%。进一步改善这一点将是一个关键挑战。

Light-Shift 2Q 门——佐治亚理工学院的工作指出了激光驱动 2Q 门的新机制的潜在优势。原则上可以应用于超精细或光学量子比特。最近的工作认为，这种

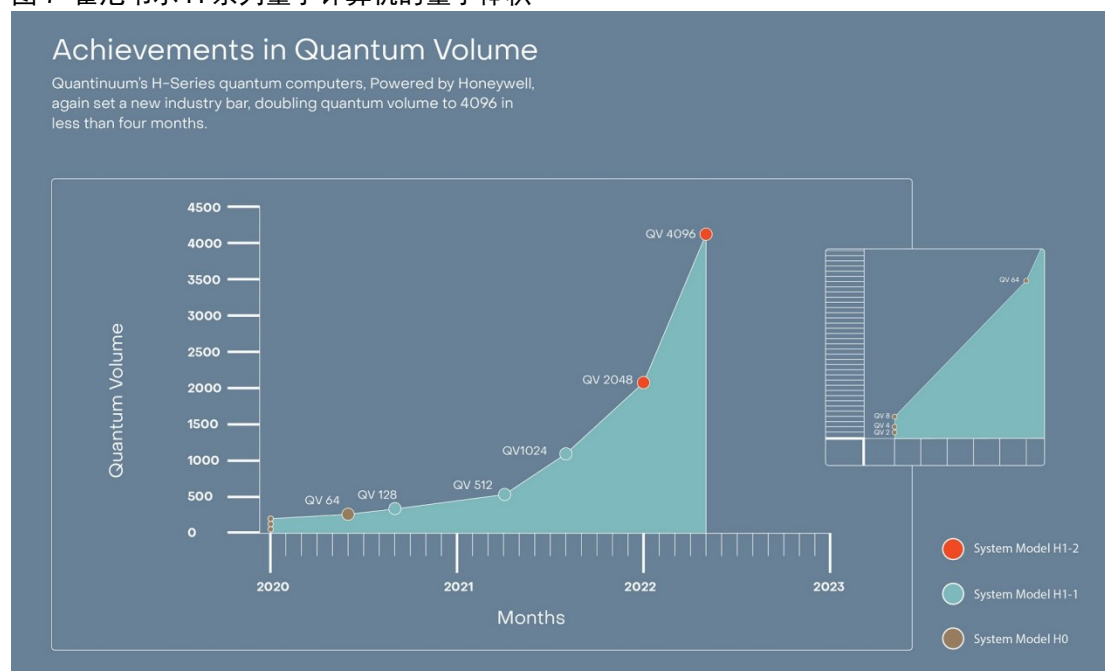
方法能够支持具有光学捕获离子量子比特的高达 99.99%保真度的门。

3、霍尼韦尔成立 Quantinuum，并继续交付产品

霍尼韦尔在 2021 年做出了一项重大的举措，将其量子计算部门剥离出来与量子软件领域的全球领导者剑桥量子公司合并，成立了一个名为 Quantinuum 的新集团。直接获得领先的软件专有技术将是最大限度地利用早期设备的一个重要优势。Quantinuum 将继续使用霍尼韦尔制造设施，Tony Uttley 继续担任新公司的总裁兼首席运营官，确保了硬件开发的连续性。

霍尼韦尔继续向外界展示他们有能力按照路线图系统地向前推进。2021 年他们再次创下记录，率先达到 1024QV，紧接着 2022 年 3 月达到 2048QV，目前最新记录为 4096QV，其目标是每年 QV 增长一个数量级。

图 7 霍尼韦尔 H 系列量子计算机的量子体积



霍尼韦尔的初步结果还显示，在 10Q 设备中成功进行了多轮纠错（使用 $[[7,1,3]]$ 色码）。霍尼韦尔利用其在中间电路测量方面的领先优势，使其能够有效地重复多轮纠错。逻辑保真度高于物理保真度（逻辑 SPAM 99.83 (2) %，物

理 SPAM 99.76 (8) %) 。

霍尼韦尔路线图——从现在到 2030 年，逐步实现 H1（线性陷阱）、H2（赛道布局）、H3（网格布局）、H4（集成光学）、H5（通过实现平铺大规模）。

霍尼韦尔的方法也与 IonQ 或 AQT 的方法大不相同。霍尼韦尔不是操纵线性离子链，而是在 QCCD 网格中重新排列离子。2021 年的其他发展为这种类型的架构指明了新的可能性。

4、离子阱互连的创新

另一家离子阱初创公司 Universal Quantum 也使用 QCCD 方法。对于提出的大规模阱离子结构，一个传统的问题是，当你已经构建了最大的可行的单个阱时该做什么。这对于小型 NISQ 应用来说可能已经足够了，但对于 FTQC 预计需要的百万量子比特设备来说，这肯定是不够的。Universal Quantum 提出了一种新的解决方案，即模块间离子的直接传输。

光子互连——将模块连贯连接在一起的标准建议是使用光子互连，实际上，支持者指出该解决方案的灵活性是整个捕获离子架构的优势。然而，到目前为止，这样的链接显示的速度是中等的（纠缠率每秒 182 次；保真度 94%）。

直接传输——在 ECTI 2021 上，来自萨塞克斯大学和 Universal Quantum 的一个团队宣布了一项引人注目的概念验证演示，即跨越微对准量子模块边界的“全电”离子传输。这大大提高了速率和传输保真度（每秒 2400 次和 99.999995%）。

直接传输不像光子传输那样灵活，但它提供了一种可以很好地结合纠错需求的工具。其他人指出，他们预计光子互连的速度将大幅提高。Entangled Networks 是一家专注于这项技术的加拿大初创公司。Aharon Brodutch（首席执行官）预计每秒 1000 次的速度是可以实现的。

5、离子阱门的创新

作为离子阱量子计算公司，Universal Quantum 继续质疑通过激光直接驱动门

的可扩展性，如在 IonQ、AQT 和霍尼韦尔系统中使用的那样。Universal Quantum 正在寻找由全局微波场驱动的门，有望带来独特的扩展优势，但前提是能够实现足够保真度的门，并能支持大量离子。

Universal 在 2021 年再次成功从 UKRI 获得了额外的赠款。一个项目将支持开发用于商业应用的纠错量子处理器，另一个项目支持与主要半导体制造商合作开发微芯片。

Oxford Ionics（牛津离子）是一家离子阱初创公司，专注于一种完全不同的近场微波方法来驱动门。它是从英国 QCS 中心分拆出来的，最近受益于一系列 UKRI 赠款，其中包括 2021 年的三笔赠款。虽然它尚未推出设备，但其创始人已经构建了一系列破纪录的实验室系统。2021 年，它一直在招聘顶尖人才。

超过 99.99%——Oxford Ionics 的联合创始人 Tom Harty 认为，离子阱有可能实现远远超过 99.99% 的保真度。“就其核心而言，该技术平台使我们能够结合我们两个最强大工具的优势：现代半导体制造技术的可重复性；以及位于原子钟核心的相同自然量子比特系统，实际上是人类有史以来建造的最精确的设备。”

Oxford Ionics 仅使用激光来控制系统的经典方面（包括冷却和读出）。Harty 指出了用微波驱动精密量子门的优势，认为相位灵敏度在这些 MHz 频率下应该更容易处理，而不是典型激光系统中的 THz。此外，微波可以提供一种超越光子散射极限的方法，这可能会使激光驱动的门难以超过 99.99%。

我们可以期待 Oxford Ionics 宣布单独的 NISQ 和 FTQC 路线图。如果可以达到足够高的 2Q 保真度，为什么还要等待纠错呢？99.99% 的 2Q 保真可能支持 100AQ 设备。那会非常有趣。

三、光子学揭示了它的另类前景

1、PsiQuantum 迈出重要一步

2021 年，PsiQ 又筹集了 4.5 亿美元，融资总额为 6.65 亿美元，估值为 30 亿

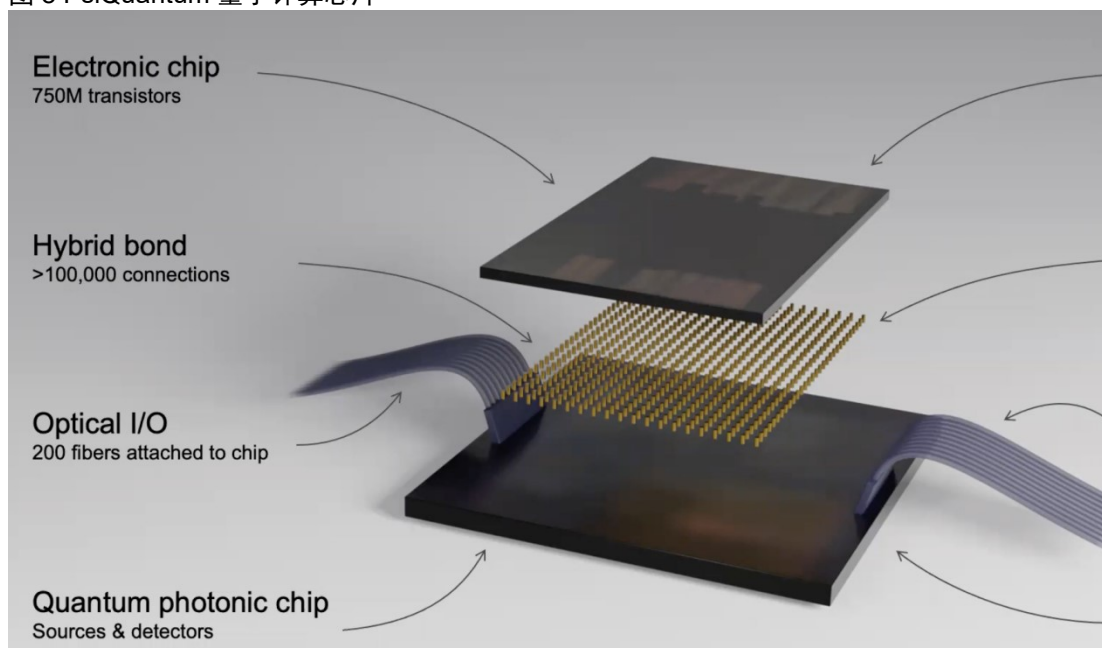
美元。PsiQ 还透露了一些具体细节。

PsiQ 已经与全球领先的半导体制造商之一 GlobalFoundries（格芯）合作了一段时间，这种合作关系已经开始显示出令人印象深刻的结果。关键的一步是将 PsiQ 的单光子源和单光子探测技术（氮化铌 SNSPD）的工具以及在线测试（基于 4K 低温恒温器）整合到格芯位于纽约州北部和德国德累斯顿的最先进的 300mm 生产设施的生产线中。

一级晶圆厂——一级晶圆厂的一个关键优势是顶级设备可以生产出更高的纳米特征精度。波导的线边缘粗糙度会导致光子损耗并降低探测器的效率。PsiQ 报告称，从精品设备到最先进的设备，图案质量提高了 5 倍，推动设备性能大幅提高（例如，单光子探测器的效率从 97%@2K 提高到了 99.7%@2K。重要的是，可以在每个晶片上制造数千个探测器以及系统所需的源、波导和其他光学组件。

PsiQ 实现了一种微妙的平衡，他们已经证明，通过利用顶级晶圆厂的能力，可以改进集成器件的关键组件。与此同时，他们避免使用奇异的材料和超尖端的制造工艺，否则他们将无法进入此类晶圆厂，这些晶圆厂的主要业务不是研发，而是传统芯片的批量生产。

图 8 PsiQuantum 量子计算芯片



Jeremy O'Brien (PsiQ 的首席执行官) 总结道：“我们没有尝试扩展量子过程，而是采用了可扩展的过程并使其成为量子。”

认为 PsiQ 的理论突破更具创新性和潜在的深远影响。PsiQ 使用单个光子来形成量子比特。他们现在已经引入了他们所谓的基于融合 (fusion) 的量子计算 (FBQC)，作为在这个体系结构中如何支持容错计算的重要简化。

基于光子路径的双轨光子量子比特——量子比特的状态 $|0\rangle$ 和 $|1\rangle$ 编码在光子所采取的路径中：它是在上波导还是下波导，还是两者都有。

在这个方案中，传统的电路模型量子计算的 2Q 门是不实用的。相反，人们经常提出一种叫做基于测量的量子计算 (MBQC) 的等效方案更实用。

MBQC 使用大的纠缠团簇态。所需的量子算法是通过团簇态的一系列测量来实现的。这种方法的一个关键挑战一直是难以产生足够大的团簇态。

FBQC 将小的标准纠缠态作为其输入。然后使用标准光子技术（贝尔测量）动态组合（融合）这些资源状态。这有效地重建了容错团簇态的能力，但关键是任何单个光子必须成功导航的光学组件的数量保持较低且恒定。

基于融合的量子计算挑战了我们对量子计算中重要事项的一些正常直觉。在传统的基于电路的方法中，我们通常关注量子比特系统的相干性必须通过增加门的数量来保护的概念。这允许量子算法利用的量子相关性在最终量子比特状态中建立。在 FBQC 中，每个单独的量子比特/光子在创建后不久都会被测量和销毁。量子相关性在与该过程控制相关的经典数据中建立。

FBQC 方法的特点是，多种形式的潜在错误（如光子损失、融合失败等）可以作为统一的错误修正过程的一部分自然解决。这与表面码等方法的核心拓扑思想密切相关。在某种意义上，FBQC 中的多轮融合类似于表面码纠错循环。从这个意义上说，两者都采用 2D 结构并增加时间步长来创建一个“3D”容错通道，计算可以沿着该通道进行。然而，制造光子结构的灵活性有望与 FBQC 方法的理论灵活性很好地结合。PsiQ 公布的“示例”架构使用 6Q 纠缠环作为它们的基本资源状态，但他们暗示这不是最佳的，使用不同的单元形状可能会提高性能。

这正是 PsiQ 团队成员所熟知的纠错理论领域。

PsiQ 方法的潜在弱点是什么？我们还没有看到运行的设备。正如其他技术一样，我们可以期待真实的经验带来对特定挑战的更加敏锐的感知。与任何 QC 平台一样，PsiQ 的量子比特最终都是模拟对象，因此必须在某些地方面对制造容差或校准的挑战。对于路径编码的光子量子比特，这可能表现出对光子相位的敏感性。串扰对其他平台来说是一个挑战，但通常被认为是光子技术的一个可能的优势。然而，从来没有人 PsiQ 现在设想的规模和组件密度下使用单个光子。PsiQ 也没有透露他们正在使用的技术来产生他们的方法所依赖的初始纠缠资源状态。每个资源状态发生器都可能需要显著的切换和复用复杂性。

经典控制——PsiQ 方法的一个优势是光子制造和控制电子制造的相对规模效果很好：大约 100 万个量子比特安装在 300 毫米晶圆上，而大约 1 万亿个晶体管安装在相同的（不同优化的）晶圆上尺寸。这种芯片可以单独制造、切割，然后使用已建立的晶圆厂工艺进行倒装芯片焊接。封装具有非常方便的控制电子/量子比特比率。

FBQC 架构的另一个显著优势是，许多基本控制处理不必在物理光子时钟周期内发生；相反，传统计算可以在多个融合循环结束后“赶上”。此功能甚至扩展到魔法态的创建，这是此处（以及大多数 FTQC 方案中）实现量子优势所需的关键资源。

在看来，经典的控制逻辑也仍然是一个观察点。PsiQ 的探测器，以及他们的整个光子芯片，仍然需要在低温恒温器温度下运行。由于 2K 比 20mK 高了 100 倍，因此比超导量子比特所面临的温度更容易工作。然而，控制逻辑的很大一部分也必须在这些低温下运行。这种低温 CMOS 技术本身仍然是一个新兴领域。诚然，许多其他量子硬件厂商都面临着这个挑战，但 PsiQ 声称它将在 21 世纪 20 年代中期建立自己的系统，因此 PsiQ 需要在这个问题上有所作为。

经典的控制逻辑，特别是产生魔法态的控制逻辑，可能是 PsiQ 的关键瓶颈。我们应该谨慎地假设快速的光子飞行时间自动意味着快速的逻辑循环时间。经典

处理的速度很可能会占主导地位。

PsiQ 路线图——100 万 Q 将在 5-8 年内提供 100-300 个逻辑量子比特。通过 FBQC 进行纠错。

从长远来看，PsiQ 希望远离 SNSPD（需要制冷）技术，这样他们的设备就可以在环境温度下运行。他们在应对这一挑战的两端都处于有利的位置——不需要低温冷却的新硬件技术（如在最新一代 QKD 解决方案中使用的）和改进的纠错协议，允许更高的错误容忍度。

2、中国科学技术大学九章 2.0 继续前进

2020 年 12 月，中国科学技术大学研制的“九章”的初步结果吸引了人们的关注。2021 年，九章得到了扩展，进一步增加了计算的复杂性，并引入了一定程度的可编程性。

图 9 中国科学技术大学九章二号



九章——以《九章算术》命名，这是一部创作于公元前 10 世纪至公元前 2 世纪的中国著名著作。最初的设备在 100 个输出模式中探测到多达 76 个输出光

子。现在已经升级到在 144 个输出模式中探测到 113 个输出光子。

中国科大 vs Google——关于正确解释九章结果的争论，很好地说明了透明竞争科学方式对各方的好处。Google 对中国科大的结果做出回应，表明在存在实验噪声的情况下，“含噪”玻色子采样可以比以往更有效地进行经典模拟。特别是，他们可以比九章更有效地重现 Scott Aaronson 最初提出的特定度量，作为对量子优越性的测试。中国科学技术大学反驳说，在九章数据中仍然存在高阶量子关联（无法用经典方法模拟）。结果是各方，甚至是 Scott Aaronson，现在都比以往更了解玻色子采样。

这不仅仅是科学上的兴趣。它给了我们一个直观的感觉，在一个噪声 NISQ 时代的设备上使用玻色子采样来证明实际有用的量子优越性是多么困难。

九章二号的真正局限性仍然在于它是基于传统光学装置中的分立元件。这种方法是不可扩展的。相反是类似于 Xanadu 或 PsiQ 所使用的方式集成组件。过去 10 年，中国大陆一直在大力投资发展半导体制造产业，从一个小参与者变成了排名前 5 的大参与者。中国科大总部所在的合肥是中国著名的 300 毫米晶圆生产中心，已有一家合肥晶合集成电路股份有限公司 Nexchip 晶圆厂投入运营，另有三家晶圆厂据报道正在规划中。

3、Xanadu 详细介绍了自己的路线

Xanadu 在 2021 年又筹集了 1 亿美元，以继续自己的光量子计算研究之旅。

Xanadu 不是使用单个光子，而是使用压缩光来形成它的量子比特。这允许使用标准 SiN 光子制造技术在芯片上组合光源和其他光子组件。只有探测器需要低温冷却，因此目前保持在芯片外。

与 PsiQ 不同的是，他们专注于为客户提供早期设备。自 2019 年推出第一个 4Q 系统以来，他们的系统规模大约每 6 个月翻一番。2021 年，他们有一个 12 模式（相当于超导系统中的量子比特）系统在线可用，一个 24 模式系统集成和一个 40 模式系统正在测试中。

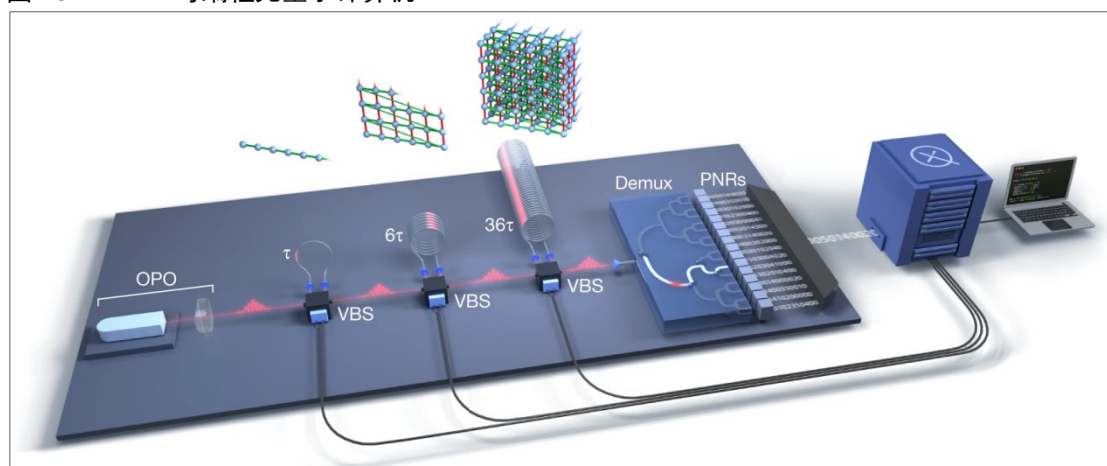
2021 年, Xanadu 公布了其通过 GKP 量子不同通往 FTQC 的独特路线图的更多细节。一个关键的优势是, 该方案在进一步的纠错之前, 已经内置了对光子损失的恢复能力。预计 FTQC 将日益成为 Xanadu 的重点。挑战包括关键瓶颈处的多路复用, 以及对运行纠错所需的经典处理的支持 (可能由 FPGA 提供)。机会包括利用增强的 3D 连接。

Xanadu 总部位于加拿大, 但与欧洲的 SiN 光子学生态系统有着密切的联系。它最近与 IMEC 合作进行芯片生产, 并与 VTT 合作生产超导光子探测器。

Xanadu 路线图——2021-23 年并行的三个处理器系列: X 系列的 X24、X40、X80; XD 系列 (100%连通性) 的 XD4、XD8、XD12、XD40、XD80; TD 系列 (时域复用) 的 TD2、TD3; 2024 年实现 5000Q 模块; 2025 年及以后, FQTC 数据中心; 通过 GKP 量子比特纠错。

2022 年 6 月, Xanadu 宣布使用其最新的可编程光量子计算机 Borealis 完成高斯玻色采样实验, 展示了量子计算优越性。该公司表示, 这是第一台提供所有门的完全可编程性以展示量子计算优越性的光量子计算机, 也是第一次通过云向公众提供具有量子优越性的机器。

图 10 Xanadu 可编程光量子计算机 Borealis



4、QuiX 继续销售处理器

QuiX 是一家荷兰初创公司，已经制造了具有 4、8、12 模式（2022 年推出 20 模式）的光子处理器，包括所需的外围控制电子设备。这些利用 SiN 光子学平台提供领先的低损耗性能。QuiX 的商业吸引力越来越大，它是少数几家实际销售量子计算硬件的公司之一。

QuiX 路线图——20×20 模式（2021 年），50×50 模式（2022 年），2023 年实现计算优势。

Orca Computing 是英国另一家基于光子学的量子计算初创公司。他们的方法强调他们专有的存储技术，这使他们在如何操纵光子状态方面具有更大的灵活性。他们将其与标准光学组件相结合，以提供一个独特的平台。这种方法的灵活性与他们在未来量子数据中心的应用中赢得的 UKRI 赠款非常匹配。

法国初创企业 Quandela 以其新型量子点单光子源技术而闻名，目前已筹集 1500 万欧元，用于建造一台光子量子计算机。最初的设备预计将在 2022 年问世。

Duality Quantum Photonics 继续保持低调。根据两位创始人 Anthony Laing 和 Alberto Politi 的记录，他们的计划将包括开发集成光子量子技术（Politi 的博士论文《集成量子光子学》（integrated quantum Photonics）在 2008 年开创了这个领域；他当时的导师是 Jeremy O'Brien）。

四、中性原子引领量子模拟

2021 年，基于中性原子的研究也继续令人兴奋。越来越多的公司正在追求这项技术，包括 ColdQuanta、QuEra、Pasqal、Atom Computing 和 M Squared。

QuEra 在 2021 年迈出了一大步，展示了一个 256 原子（量子比特）的量子模拟器。这个 2D 冷原子阵列还没有实现完整的量子比特门集，但它已经可以被编程来重现类似量子系统的动力学。这些结果已经引起了科学上的兴趣，并可能有更广泛的应用。

Pasqal 是一家法国初创公司，也在走这条道路。它的创始人展示了一个 200 原子的模拟量子模拟器。Pasqal 的工作重点是强调通过这种模式在脉冲控制和算法层方面可以实现的目标，以及向门模型设备发展。

另一家走上这条道路的初创公司 Atom Computing 推出了 100 原子模拟器，并在 2021 年进行了高调招聘。

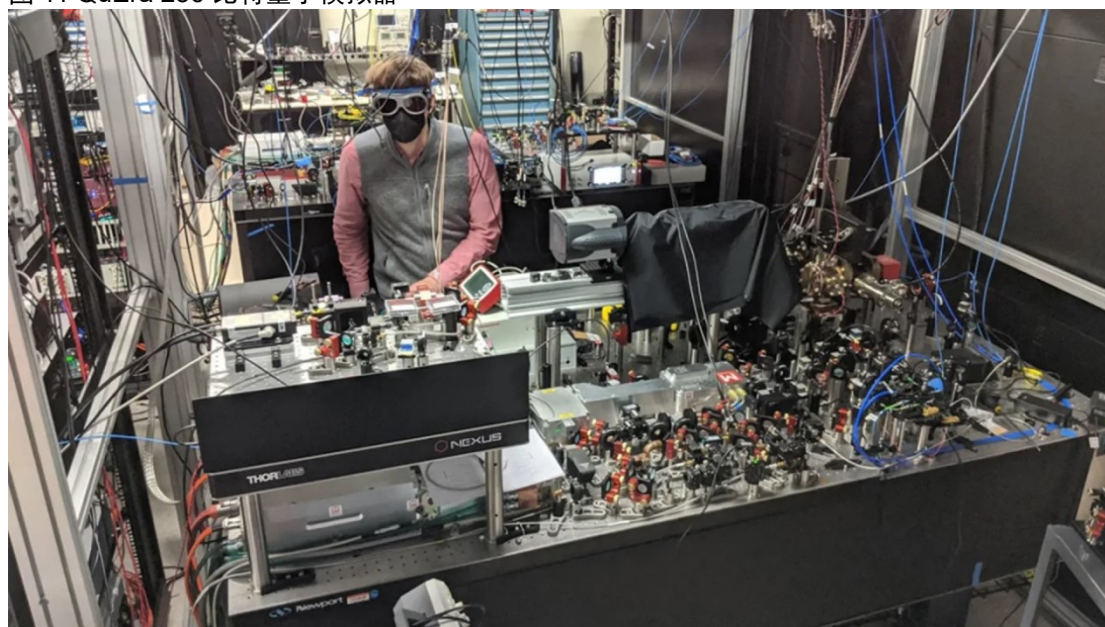
ColdQuanta 一直是中性原子技术的早期领导者。DARPA 的 ONISQ 项目支持将这项技术作为量子计算基础的工作。它似乎无法在 2021 年实现 100Q 云设备的目标，但现在预计这一目标将在 2022 年初实现。

QuEra 路线图——256 原子模拟器 (2021 年)、64Q 量子计算机 (2022 年)、1024Q (2024 年)；使用 Steane-7 进行纠错

Pasqal 路线图——200 原子模拟器 (2021 年)、1000Q (2023 年)

ColdQuanta 路线图——H1 100Q 4X 连接 (2021 年)、H2 200Q 8X、H3 300Q 20X、H4 1000Q 50X (2024 年)、H5 2000Q+ 60X+

图 11 QuEra 256 比特量子模拟器



中性原子系统已经在量子模拟器方面占了先机。其性质也为将其扩展到 1000Q 提供了一条清晰的路径。除此之外，ColdQuanta 还设想，在 1 平方毫米的

空间中，一台 10 万 Q 的设备是可能的，不过他们也承认，管理所需光学系统的复杂性将是一个巨大的挑战。

这种系统作为通用门模型量子计算机运行的潜力在 2021 年也得到了提升，加州理工学院演示了 99.1% 的 2Q 门保真度。这使用了原子的高度激发态“里德堡态”。读取时间特别是复位周期时间，可能也是这项技术的一个挑战。一般来说，中性原子还没有建立起 FTQC 的技术路径。

重要的是要意识到中性原子技术在量子技术生态系统的其他领域，特别是在量子传感领域具有强大的影响力。这为该领域的参与者提供了选择多样性和支持机会。

以其高性能激光器而闻名的 M Squared 已经建立了强大的地位，使这项技术能够用于量子传感。2021 年，它还开始构建自己的量子计算系统。

五、硅自旋量子比特实现三次飞跃

硅自旋量子比特长期以来一直具有吸引力。同位素纯化的 ^{28}Si 提供了一个“自旋真空”，可以在其中容纳精细的自旋量子比特。它还承诺利用为半导体行业开发的制造技术。然而，使用精密自旋量子比特实现的保真度落后于其他平台。

在硅自旋量子比特向前迈出的一大步，三个团队现已公布了超过 99% 的 2Q 门保真度的结果。

QuTech 已经在 2Q 测试装置（一个门定义的双量子点在一个同位素富集的 $^{28}\text{Si}/\text{SiGe}$ 异质结构）中证明了 99.5% 的 2Q 门保真度。连接两个这样的量子点的能力也在中得到了证明。

日本理化学研究所（RIKEN）在一种 2Q 测试装置（同样是同位素富集的 $^{28}\text{Si}/\text{SiGe}$ 异质结构中的三重量子点）中，证明了 99.5% 的 2Q 门保真度。

新南威尔士大学（UNSW）已经在 3Q 测试装置中证明了 99.37% 的 2Q 门保真度。硅器件上的一对离子注入的 ^{31}P （磷）核允许一个电子自旋和两个核自旋耦合。这是施主量子比特可扩展性概念的真正证明。

这些结果的技术和地理多样性是半导体量子比特平台潜力的显著标志。学术团体正在探索的大量技术并不总是相互兼容的，但它们共同代表了一种可能性的力量。

2021 年还展示了其他几项有趣的技术。

由全局微波场驱动自旋量子比特门——新南威尔士大学展示了自旋量子比特门，其使用的技术与一些离子阱团队所采用的技术相同，因为它具有潜在的扩展优势。这种技术传统上利用“缀饰态”来抑制对磁场噪声的敏感性。在追求硅技术的过程中，UNSW 的团队引入了一种新的增强型“SMART”协议，有望抑制更高阶的噪声。

锗——另一种方法是基于硅晶片上锗层中的空穴（而不是电子）来定义量子比特。这正迅速成为一个有前途的平台：第一个锗量子比特于 2019 年实现，2020 年实现了两个量子比特，2021 年实现了一个四量子比特系统。锗的进步证明了半导体技术可用于在二维阵列中扩展量子比特的概念。

Photonic Inc——继续致力于将光子互连引入硅自旋平台。

英特尔在 2021 年提醒大家要关注他们在自旋量子比特方面的长期潜力。在与 QuTech 的合作中，英特尔演示了在最先进的 300 毫米晶圆厂中制造量子点阵列。概念器件的初步验证已经达到了与以前的测试器件相比的 1Q 门保真度和相干寿命。扩大规模的潜力是诱人的。正如英特尔所说，量子点实际上就像晶体管的极端单电子情况。另一方面，大型设备中潜在的串扰问题还没有得到研究。

光刻——英特尔认为严格遵守晶圆厂设计规则是实现所需极高产量的关键。特别是，它使用全光学光刻（包括化学机械抛光），而不是目前用于量子点制造的电子束光刻。一个 300 毫米晶圆包含 1 万个量子点阵列，每片晶圆多达 55 个门。

Cryo-CMOS——英特尔和 QuTech 也成功地对最新的 Horse Ridge 控制芯片进行了基准测试，该芯片能够在 3K 下运行，以驱动量子比特的微波控制。

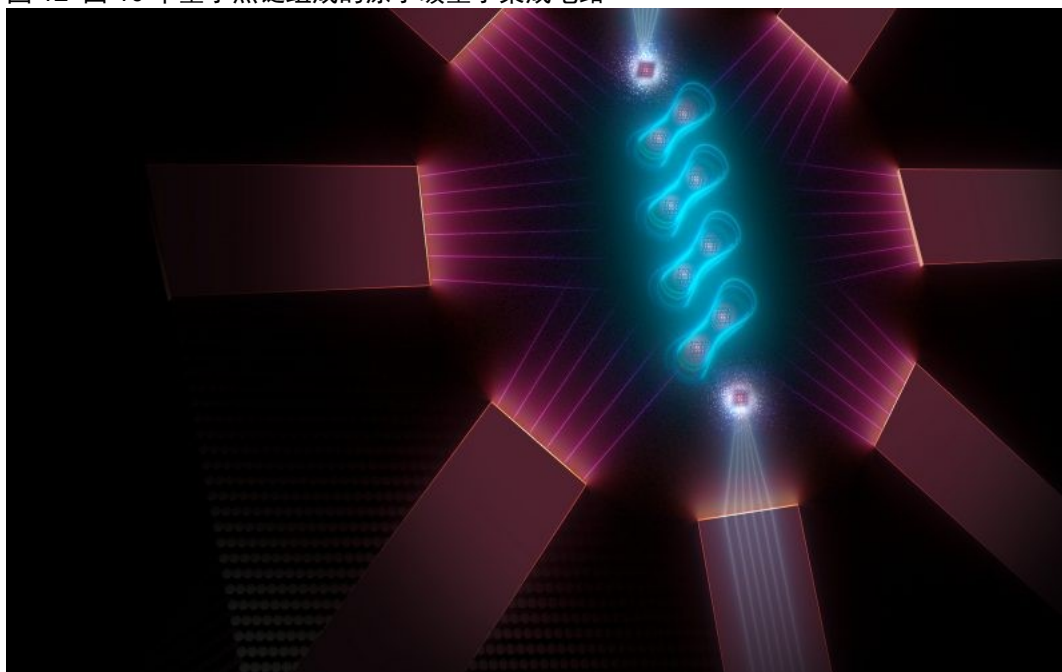
SQC 可能是最著名的硅量子比特初创公司。然而，它使用了一种非常不同

的技术：硅中的磷原子量子比特。这些器件使用超尖端技术制造，提供了超越传统 CMOS 技术的原子精度。我们还需要等待一段时间，才能看到他们的愿景是否真的能跨越这一领域。

SQC 路线图——2023 年 10Q 原型，2030 年 100Q，到 21 世纪 30 年代中期实现有用的 FTQC。

2022 年 6 月，SQC 和新南威尔士大学宣布推出世界上第一个在原子尺度上制造的量子集成电路，由 10 个量子点链组成。他们使用这种量子处理器准确地模拟了有机化合物聚乙炔的结构和能量状态，最终证明了该团队技术的有效性。

图 12 由 10 个量子点链组成的原子级量子集成电路



在欧洲，QLSI 项目的启动对硅自旋支持者来说是一个重大推动，它吸收了 CEA-Leti、CNRS、IMEC 和其他公司的专业知识。主要目标包括通过 QuTech 的 Quantum Inspire 开放访问平台提供 8Q 处理器，并在 2023 年之前展示 16Q 芯片。

英国硅自旋初创公司 Quantum Motion 有望从 QLSI 中受益。它还获得了 UKRI 的资助，用于开发用于控制和读出的低温 CMOS 解决方案。

六、NV 色心有其独特的潜力

金刚石中的 NV 色心是另一个量子信息平台。12C 没有核自旋，因此形成了量子比特系统的磁中性主体。金刚石还具有良好的热性能，这意味着设备即使在室温下也能保持性能（尽管在较低温度下保真度会提高）。门的保真度仍然是一个挑战。然而，与单个缺陷相关的多个 13C 核自旋可以提供高保真性能。这个平台良好的光学特性意味着它经常被认为是量子互联网上小型处理器节点的候选。

QuTech——在 2021 年的一次演示中，纠缠态分布在三个 NV 节点（冷却到 4K 温度）之间。每一个都包含一个用于通信的量子比特。中间节点也使用 13C 的核自旋作为存储量子比特。

Quantum Brilliance 是一家澳大利亚初创公司，基于金刚石 NV 构建室温量子计算机。他们的第一代桌面系统已经上市。

金刚石 NV 的卓越特性也使其能够在量子传感领域取得快速进展。我们可以期待听到更多关于这项技术的信息。

澳大利亚材料技术公司 Archer 也一直在为进入量子技术市场做准备。其碳纳米球技术为自旋量子比特提供了一种新的基底选择，但仍处于发展的早期阶段。室温下（175ns @ 300K）的量子比特寿命比金刚石 NV 短，但该平台有望带来新的制造灵活性。量子比特逻辑运算尚未得到演示。Archer 在亚洲、欧洲和美国获得了一系列专利。

C12 量子电子公司正在同位素纯化的碳纳米管中构建自旋量子比特。同样，制造灵活性是一个关键优势。预计操作将针对稀释制冷机系统以获得最佳性能。

EeroQ 正在开发另一种新形式的自旋量子比特，其基于被液氮捕获的电子。其发展还处于早期阶段。

六、猫量子比特开始成形

AWS 团队在量子纠错方面拥有非常强大的平台实力。一个结果是针对 FTQC 架构提出越来越详细的建议，其开销显著降低，尤其是通过猫量子比特。其他工作指向更有效的技术，用于实际表面码实现。

Alice & Bob 是一家法国初创公司，已经走上了实现猫量子比特的道路。

七、正确的事情

这场竞赛将继续推出足够强大的设备，以释放量子计算的巨大潜力。虽然已经出现了明确的领导者，但每个人都面临着非常不同的规模挑战。目前还不清楚哪个主要的量子比特技术平台会在 NISQ 或 FTQC 时代获得成功。量子互联网上 FQCC 应用的赢家可能会再次不同，如果商业 NISQ 应用的进展停滞，这可能会变得更加重要。每一项仍在开发中的技术的多样性为初创公司留下了巨大的施展空间。

认为，提供潜在的量子比特性能现在是最重要的。用电路模型的术语来说，99.9% 的 2Q 门保真度将成为最低标准，而对于那些在 NISQ 时代寻求广泛量子优势的人来说，甚至需要 99.99%+。单独的门的的结果是不够的（即使通过随机基准测试进行验证）。我们需要在大型设备上看到与门同时操作的结果（通过先进的技术，如周期基准测试来验证）。

对于那些想要尝试 FTQC 的人，你需要能够非常清楚地解释你的纠错方法是如何工作的，不仅是在原则上，还包括真实设备中出现的错误。量子硬件需要扩展，但所需的经典控制硬件也需要扩展。

传统的电路模型领域也需要明白，这并不是唯一的戏。量子退火等启发式方法有显著的发展势头。在物理学的专业应用之外，模拟量子模拟实际上仍然是未被探索的。简单的“少量子比特”设备可以在量子互联网上有新的应用。也许最具颠覆性的是，新的纠错方法，例如 FBQC，可能是我们超越传统范式思考可以

实现的目标的指针。

量子未来是光明的，但它仍然充满不确定性。

八、展望 2022

- IBM——127Q Eagle 会加入“超越经典”的俱乐部吗？
- 谷歌——我们会看到表面码的进一步发展吗？
- Rigetti——为英国开发的新量子计算机的规格是什么？
- 祖冲之系列——中国会在纠错和容错方面领先吗？
- 本源量子——中国大型超导量子比特设备会影响云端吗？
- OQC——新款 8Q 云处理器会有哪些性能数据？
- IonQ——其第二代铯离子处理器的 QV 能达到多高？另请关注第三代钡离子处理器的早期性能结果。
- AQT——“世界上最小的 QC”的下一步是什么方向？
- 霍尼韦尔——关注通用门集的纠错演示。
- Universal Quantum——其高磁场芯片正在工作；它们能达到什么保真度？
- 牛津离子——我们会看到第一个近场微波离子阱装置进入比赛吗？
- PsiQ——我们会听到更多关于他们承诺出售的纠缠源的信息吗？
- QuiX——20×20 模式设备的发布。我们将看到哪些性能信息？
- Xanadu——他们的 24×12 模式设备刚刚上线；是时候进行模式指标之战了吗？
- 九章系列——关注中国科学技术大学专家更倾向哪种光子学平台
- SEEQC——我们什么时候才能第一次看到其 SFQ 技术的实际应用？
- 中性原子——原子模拟器或门模型设备会统治中性原子云吗？
- 硅自旋——我们会看到朝着真正的多量子比特阵列取得进展吗？
- 金刚石——我们会看到独特的 FQQC 应用程序的进展吗？
- 猫量子比特——Alice & Bob 会把猫量子比特提上议事日程吗？我们会看到

AWS 的第一批硬件的性能数据吗？我们会看到来自 QCI 一流团队的猫量子比特吗？

- 拓扑量子比特——在 2020/21 年挫折之后；故事还能向前发展吗？（2022 年 3 月已经取得进展）
- 创新——关注来自新兴参与者如 EeroQ、Archer 或 C12 的量子比特控制逻辑演示。
- 欧盟 QT 旗舰——下一轮 Horizon Europe 项目将产生哪些赢家？
- 英国 NQCC——新的国家量子计算中心将最终开放。它选择支持的技术将是更广泛进步的晴雨表。
- 美国 NQI——NSF 和 DOE 国家实验室中心将取得哪些新进展？
- CEA-Leti——这个主要技能中心能开始加速硅旋转量子比特之旅吗？
- QuTech——我们将在 Quantum Inspire 上看到哪些新处理器？
- 中国——我们还会看到关于离子阱或中性原子系统的“追赶”演示吗？
- 指标——不要指望离子阱支持者会像接受 QV 一样迅速地采用 CLOPS；但是用户至少可以坚持使用新的 QED-C 基准套件？
- 保真度——谁有能力令人信服地跨越 99.9% 的 2Q 保真度门槛？

第二章 量子算法展望

量子计算机的早期应用看起来并不成熟。但潜力确实存在。开发量子算法的人才团队仍在为早日实现真正广泛的量子优势而努力。那么可以实现什么？什么时候能实现？

量子计算机从它们运行的独特的量子算法中寻求优势。在某些情况下，这些方法比传统方法有显著的（指数）加速作用，而在其他情况下则是较有限的（平方）加速。某些情况下，诸如量子随机性之类的独特属性会提供不同的优势吗？

关于量子信息处理技术的研究已经超过 25 年。即使在没有实际设备的情况下，取得的进展也是显著的。

然而，研究时间最长的算法通常需要全尺寸 FTQC 机器，即使在目前的技术水平下，这仍然很难实现。2021 年，许多研究方向再次集中在近期 NISQ 设备的算法可能实现的目标上，或早期 FTQC 设备可能实现的目标上。

随着人们对量子计算的兴趣迅速增加，企业提出了一些关键问题：

- 1-2 年——早期量子设备将首先从哪个方面进入日常业务运营用途？

大众炒作可能会让它听起来像是已经发生了一样。然而仍然没有看到在商业应用中日常生产使用的例子。

- 3-5 年——在 NISQ 时代，可能会解决哪些重要的商业应用？

虽然我们有理由对特定的用例保持乐观，但跨越一系列业务问题实现广泛的量子优势的目标仍然有许多难以克服的障碍。

- 7-10 年——早期 FTQC 设备可能会解决哪些应用？

对于当前这一代领先的架构，答案比我们希望的要乐观，但重要的应用正在清晰地显现出来。

- 长期——围绕量子计算的炒作合理吗？

认为，关于量子计算的长期预测仍然是非常光明的。

一、我们实现了什么？

量子云已经不是什么新鲜事了。自 2016 年起就可以通过 IBM Quantum 进行访问。从 2019 年的谷歌，到 2020 年和 2021 年的中国科大，其相关成果都展示了“量子计算优越性”。

众多的研究成果是量子专家和行业早期实践者们进行头脑风暴的见证。他们讨论的基调似乎经常表明量子应用现在正在加紧部署。但事实却不尽如此。

D-Wave 已经实现了大量的概念应用证明，包括单个真实世界的演示，如 2019 年在里斯本优化公交线路。许多客户肯定会说，他们已经通过发展团队和将量子启发的知识应用到他们的业务中而在商业上受益。然而，蓝筹终端用户在日常生产活动中对量子应用的使用仍然是难以捉摸的。

在 2021 年的 Qubits 会议上，Catherine McGeoch（D-Wave 高级科学家）评论道：“D-Wave 在量子处理器的常规速度足以克服日常开销之前，我们不会声称拥有量子优势。我们还没有达到目标，但我们知道如何达到目标。”

量子退火的应用很快就会投入生产使用；然而，它也面临着传统设备的持续竞争，这些设备运行着量子启发算法的高效实现。

Google 认为他们可能接近于“量子加扰”（Quantum scrambling）的应用。量子系统中量子加扰如何传播的动力学尚不清楚。对这里更好的理解可以应用于理论物理学（也许以后会更广泛地产生连锁反应）。可以使用类似于 Google 首创的随机电路框架的实验装置来研究这些影响。

Phasecraft 发表了一份关于如何模拟 Kagome 磁体的文章，表明具有 50 个量子比特的系统可以通过具有 200 个以下 2Q 门的量子电路来解决。这似乎即将通过当前一代 NISQ 设备实现。了解这种自旋液体基态并没有直接的商业应用，但它是理论物理学中一个众所周知且重要的领域。

Google 和 Phasecraft 的提议之所以引人注目，是因为它们采用了灵活的门模型量子计算。然而，如果我们允许在理论物理中应用，那么基于中性原子的模拟

量子模拟器可以说已经这样做了好几年了。

剑桥量子可能即将通过其 Quantum Origin 网络安全 SaaS 产品（以前称为 IronBridge）实现真正的商业部署。这为加密密钥（以及其他需要真正无偏随机性的应用）提供了随机数。通过实施强大的实时熵验证（通过贝尔测试），它提供了当前任何其他 QRNG 都不匹配的功能，这在传统设备上是不可能的。

从中期来看，此类服务可能会使用低成本的专用设备。然而，Quantum Origin 现在已经可以商用（了解到价格非常适中）。谁先购买并部署它，就可以说他们将第一个量子应用投入正常生产！

剑桥量子最近与霍尼韦尔合并，组成了 Quantinuum。在初始运行阶段，Quantum Origin 将由 H 系列霍尼韦尔量子计算机提供服务。

随机数仍然是早期应用的一个重要机会。重要的一点是，算法可以为原始的随机性增加价值。在密码学中，我们通常希望最小化我们必须信任的人。Quantum Origin 在软件中提供了强大的熵验证。用户将不再需要信任设备的制造商，尽管仍然需要信任操作人员。之后听到越来越多关于量子随机数的消息，我们不应该感到惊讶。

图 13 量子随机数平台 Quantum Origin



可公开认证的随机数——此类服务的另一个目标是可以公开和远程进行的熵验证。我们知道如何使用 FTQC 结合 PQC。然而，目前在 NISQ 设备上实现面临着障碍，即我们目前拥有的最佳协议需要验证检查，这是一个数学难题，使其不切实际。这方面的进展将开启一系列有趣的新应用，包括权益证明区块链协议。

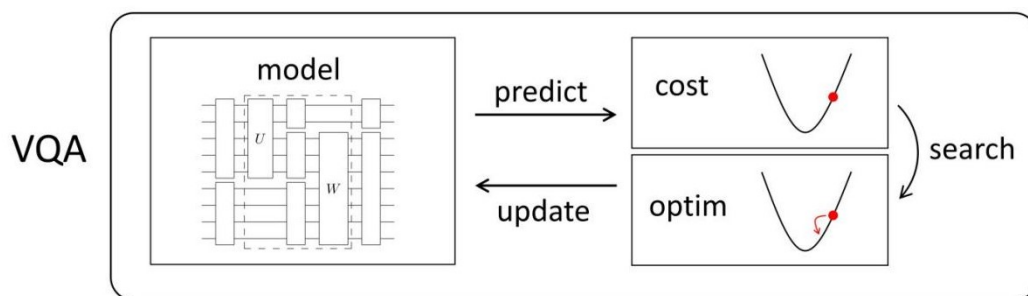
二、寻找广泛的量子优势

量子计算专家、学术团体和越来越多的初创公司，一直在努力提前量子计算实现更广泛优势的日期。变分量子算法、量子退火、蒙特卡罗技术的应用和量子机器学习都是活跃的重点领域。

1、变分量子算法

变分量子算法（VQA），包括 VQE、VQS、QAOA、QCBM、QNN 及其日益复杂的改进，已逐渐成熟，成为最适合使用门模型 NISQ 计算机实现量子优势的相关技术体系。

图 14 变分量子算法示意图



混合量子-经典循环——实际实现正在寻求平衡迭代处理循环的竞争需求：为初始试验输入（ansatz）选择一个好的模型；选择一个成本函数，既要具有量子硬件效率，又要适合具体问题；减少噪音和错误；有效地测量输出；将尽可能多的工作量纳入经典后处理；运行高效的经典优化程序来驱动每次迭代。

1) 变分算法的风口

研究越来越集中在确定以足够的规模和准确度运行应用程序所需的实际资源，以解决感兴趣的现实世界问题。目前来说，以下两个挑战成为重大障碍：如何有效地测量每个周期中的量子输出以及驱动变分优化过程的问题。

VQE（变分量子本征求解器）是一系列技术，为在计算化学等领域进行计算提供了希望。最近的工作已经确定了这个过程中的一个关键瓶颈。为了达到通常所需的精度水平，必须对每个试验电路进行重复的输出测量。所需的大量重复看起来像是一个严重的瓶颈，有可能将运行时间超出可用性的范围。虽然这个问题首先在 VQE 中浮出水面，但随着我们更好地了解它们对准确性的需求，它有可能影响其他变分算法。

Zapata 完成了一系列短链碳氢化合物（从甲烷到丙炔）的运行时间估算工作。使用传统的 VQE 方法，他们估计每次所需的优化迭代的运行时间为 2 到 71 天。将需要多次迭代，对于其他感兴趣的分子，时间可能会明显更长。这使得 VQE 在没有某种方法来减轻测量负担的情况下看起来不可行。

Zapata 引入了鲁棒振幅估计（RAE）技术作为缩小这一差距的第一步。振幅估计是估计量子态上可观察量的关键技术，量子态是 VQE 的关键组成部分。RAE 有助于我们在嘈杂的量子处理器上使用这种技术。

荷兰量子软件初创公司 Qu & Co 与传统计算化学软件专家 Schrödinger 公司合作。他们的工作受益于对量子计算潜力以及当前经典方法优缺点的深刻洞察。他们的工作质疑 NISQ 时代实施的 VQE 是否有望达到化学精度（通常被视为 1kcal/mol 或 1.6mH）。一个普遍的观察是，迄今为止，许多量子演示都将准确性与精度混为一谈：他们计算出精确的结果，但模拟的轨道太少，无法达到真正的准确性。

Zapata 开发了一种“经典提升”VQE 的技术，允许使用传统的近似计算一些轨道，而量子处理器只处理那些具有强量子相关性的轨道。

变分算法的另一个普遍挑战是确保所需的经典优化能够有效地完成。在许多

情况下，这类似于我们沿着斜坡寻找最低点（最优解决方案），而我们却有可能找到一个空洞（局部极小值），而这并不是最佳的整体解决方案。如果我们发现自己在一个非常平坦的地方（贫瘠的高原），那么我们可能不容易知道下一步该走哪条路。设备的噪声也可能使一个微妙的斜坡变成贫瘠的地形。

NP-hard——2021 年的工作巩固了我们对这个问题的理论理解。不幸的是，在一般情况下，VQA 面临的优化挑战是一个 NP-hard 问题。

威胁在于优化的经典成本可能超过量子加速。最坏的情况很难，这不应该让我们过分担心。特别是当我们模拟一个物理量子系统时，我们可以使用物理或化学的洞察力来选择一个试验解和近似的哈密顿量。我们可以有一种直觉，我们的量子系统将帮助我们找到自然的解。

然而，当我们处理一般优化问题时，我们的直觉可能不那么强烈，这可能会通过诸如 QAOA（量子近似优化算法）之类的方法来解决。在这里我们可能需要更具体的理由来认为我们选择的试验解和成本函数给了我们一条简化的优化路径。

D-Wave 迅速指出了这种推理给了 QUBO 和量子退火的支持，这是 NISQ 时代优化问题的首选策略。

纠缠诱导的贫瘠高原——可见层和隐藏层是传统深度学习的基本组成部分。最近的研究表明，可见和隐藏的单位之间的过度纠缠会导致贫瘠高原和训练失败。虽然这令人沮丧，但它也可能指出了避免这个问题的方法。

Zapata 开发了一个开源工具 orqviz，通过帮助优化环境的可视化来帮助解决优化挑战。

2) 变分算法的进展

NISQ 时代的量子优势主要集中在几个领域。其中特别包括在化学和材料科学中的应用。这些系统潜在的量子本质支持了我们的信念，即量子计算可以帮助我们探测它们的属性。

分子结构——VQE 用于计算感兴趣分子的基态（或激发态）能量。这一领域的技术正在快速创新。

Zapata、剑桥量子、Phasecraft、QC Ware、Rahko、QunaSys 等都是利用学术人才推动创新的初创企业，每家公司都提供 VQE 的变体和改进。

剑桥量子和罗氏已将密度矩阵嵌入理论的传统计算化学技术与 VQE 相结合，以检查蛋白质-配体结合能，计算是在 IBM 和霍尼韦尔处理器上进行的。

材料科学——传统方法通常只能处理量子相关性较弱的材料。理解规则晶格阵列是一类重要的问题，通常以费米-哈伯德模型为特征。这包括可能具有很高实际重要性的系统，如理解高温超导性或电池性能。

Phasecraft 提出了一种优化的变分算法来计算 2D 费米-哈伯德模型中的基态能量。可以在具有大约 325 个 2Q 门（在完全连接的架构上）的 50Q 设备上处理 5×5 实例（比经典方法所能精确求解的要大）。

Rahko 所采用的方法首先关注最先进的方法（例如动态平均场理论）可以在 HPC 平台上实现的程度。它后来计划使用基于 VQE 的技术来增强这些功能。

分子动力学——计算化学中传统方法很难处理电子激发的时间动力学。这种动力学可能与光伏和发光二极管的应用有关。VQS（变分量子模拟）技术旨在解决这一领域。

Phasecraft 在 5×5 晶格上模拟费米-哈伯德模型模型中的时间动力学的工作仅提出了 3,209 个 2Q 门和 259 个时间步长。这低于使用原生量子比特操作的传统电路模型，并将错误缓解技术构建到算法中。

专利——Phasecraft 已经为其将费米子映射（编码）到量子比特以进行此类量子计算的有效方法申请了专利。

优化——Grover 搜索算法原则上可以为许多组合优化问题提供平方加速。然而，高资源需求使其远远超出了 NISQ 设备的能力范围（正如我们将看到的，可能也超出了当前 FTQC 架构的能力范围）。QAOA 是一种 VQA，已经被许多团队研究用于基于门模型的 NISQ 应用。没有普遍的证据表明它比经典方法更有优

势，所以重要的是要有一些直觉，为什么量子实现可能有助于手头的具体问题。

困难 vs 容易——最近的工作让我们能够更清楚地了解 QAOA 在困难（例如 3-SAT）和简单（例如 2-SAT）问题上的表现。这可以为更好地直观地了解它可以提供的好处指明方向。

IBM 展示了探索如何将组合优化问题映射到局部量子哈密顿量的工作。这使我们能够将他们的解视为类似于寻找哈密顿量的基态，使用 VQE 或量子相位估计等技术。

在没有完全纠错的情况下，研究团队通常会应用其他错误缓解技术来最大限度地发挥 NISQ 处理器的能力。这些技术通常基于控制硬件或控制软件。算法设计也有其作用。可能需要针对特定设备的优化。

作为英国 UKRI/加拿大联合资助计划的一部分，两家公司 Phasecraft 和 Quantum Benchmark 正在与加拿大量子计算研究所(IQC)和伦敦大学学院(UCL)合作开发容错算法。

2、用于组合优化的量子退火

各种各样的业务问题都可以定义为组合优化问题。这些范围从金融服务中的投资组合优化到旅行推销员问题(它概括了运输、物流和制造中的许多常见问题)。

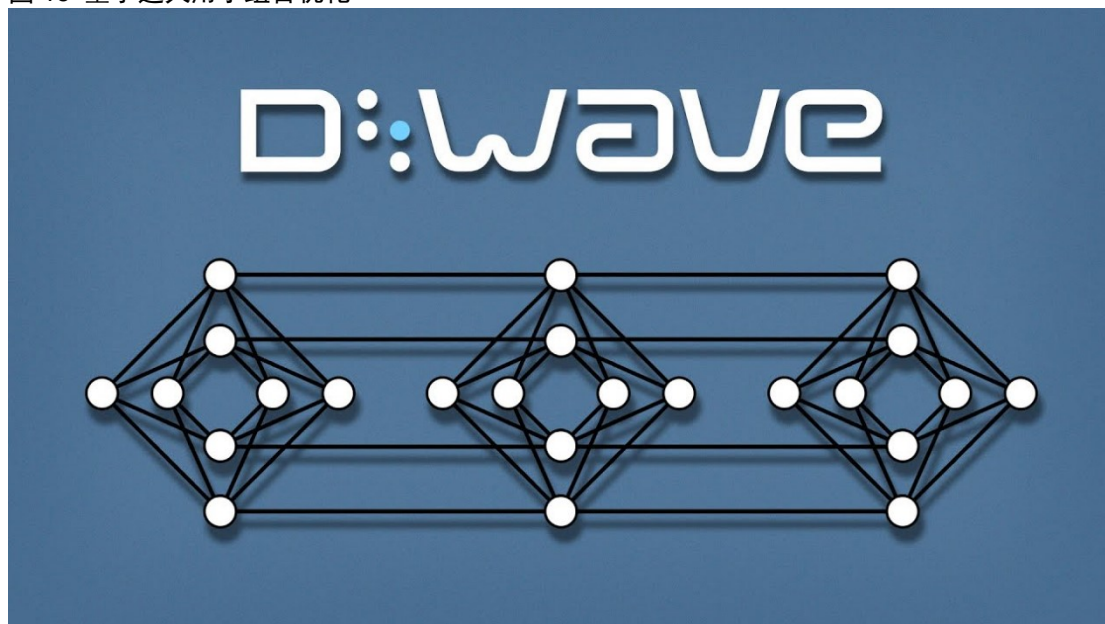
QUBO (二次无约束二进制优化) 是基于量子退火设备固有的组合优化模型。在这里，我们有一个直觉，即量子隧穿效应可以帮助避免输出被困在次优解中。最近，原则上表明 D-Wave (“随机”退火) 使用的架构确实可以提供加速 (尽管证明确实假设了无噪声设备和有利的问题选择)。关于我们对当前设备中可用的嘈杂、短相干时间量子比特的期望，学术辩论仍在继续。

Paypal 已经使用深度学习技术进行欺诈检测。然而，这些算法的特征选择是一个重要的组合问题。Paypal 正在与 D-Wave 合作，比较基于 QUBO 的模型和用于特征选择的经典模型。

Multiverse Computing 之前曾使用 QAOA 和量子退火与 BBVA 一起探索金融

服务组合优化任务，后者表现更好。最近，他们扩展了这项工作，显示了使用标准普尔 500 指数的真实资产优化金融投资组合的有希望的结果。这使用了 D-Wave 混合工具及其 Advantage 量子处理器。

图 15 量子退火用于组合优化



来自富士通、东芝、日立和 NEC 的数字退火机继续为这些方法提供量子启发的竞争。

东芝一直在追求量子启发的优势，利用模拟分岔算法（SBM）解决问题。它的 SBM 是一个适合在传统高性能硬件上运行的软件包。它已被证明可以解决多达 10 亿个二进制变量的问题。

微软的工作指出，由于在当前架构中嵌入 QUBO 问题时连接性约束引起的开销，量子退火相对于数字退火面临扩展劣势。

Zapata 开发了一种量子增强优化技术，该技术采用生成式建模来寻找组合优化问题的更好解。该方法的优点是不同于 QUBO 问题，并且可以利用经典和量子机器学习模型。他们首先将其证明为标准普尔 500 指数投资组合优化的量子启发模型。

3、量子加速蒙特卡洛技术

传统蒙特卡罗技术在工商业中得到广泛应用。特别是，这些技术在金融服务行业中被广泛用于衍生品定价、信用估值和风险管理。量子蒙特卡罗技术(QMC)有望加速这些非常有用的计算。这些取决于振幅估计。

QC Ware 已经减少了从 QMC 中获益所需的资源需求。这减少了电路深度，但增加了迭代，这种权衡降低了量子速度，但使其实现更近了一步。

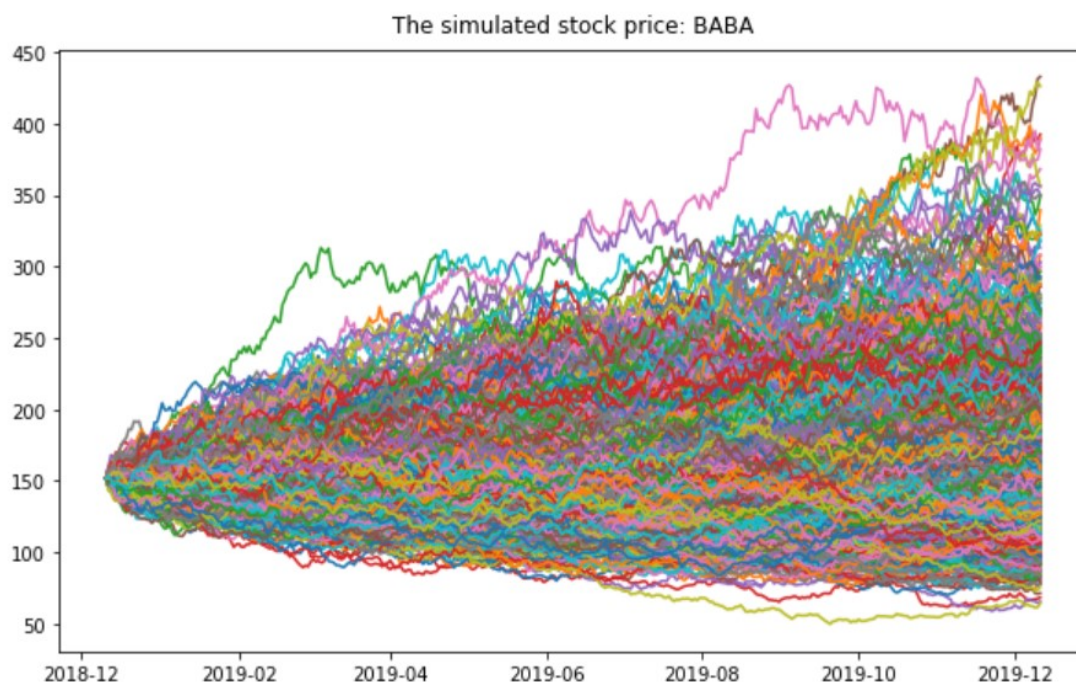
QC Ware 获得了低电路深度振幅估计技术和高效数据加载技术的专利。

QC Ware 已经在 IonQ 的最新硬件上完成了一个概念演示证明。它使用一元编码和 4 个量子比特，电路多达 92 个 2Q 门，电路深度为 62。

算法创新正在使量子优势更接近实现。然而，仍然存在重大障碍。QC Ware 已根据 2Q 门保真度和有效时钟速度估计了在实际衍生定价用例中获益所需的资源需求。这表明我们仍然需要在门保真度上进一步提高几个数量级；此外，时钟速度可能是当前离子阱架构无法克服的挑战。

高盛和 IBM 计算出了衍生品定价中量子优势的一个阈值。这始于商业洞察力，即具有路径依赖敏感性的衍生品将首先从量子方法中受益。当设备能够提供 8000 个逻辑量子比特和足够的逻辑保真度来支持 10^{10} 个逻辑操作时，他们预见到商业利益。这将需要使用纠错，在这项初步工作中，所需的逻辑时钟速率为 10MHz，与当前的 FTQC 架构预期提供的相比，看起来非常激进。高盛和 IBM 提出了新的技术，可以将逻辑时钟速率要求降低到大约 30kHz（更接近早期 FTQC 架构设想的 10kHz）。

图 16 阿里巴巴股价的蒙特卡罗模拟



4、量子机器学习

传统的机器学习已经在商业领域获得了广泛的应用。量子机器学习，也许比量子计算的任何其他领域都更受到关注。要想从炒作中探出真相，我们必须清楚为什么我们期待量子带来优势。

反量化(De-Quantization)——进程并不总是一帆风顺的。Kerenidis 和 Prakash 的推荐系统最初虽然提供了指数级加速，但后来改进的经典算法将其简化为（仍然相当可观的）多项式之一。同样的方法也影响了其他流行的机器学习技术的量子算法，包括主成分分析和最近质心聚类。

1) 加快运算速度

量子可以提供帮助的一个明显方式就是加速经典技术。HHL 允许对线性代数进行非常普遍的加速，但仅适用于本机量子数据和输出。Grover 算法允许在许多非结构化搜索应用程序中实现非常普遍的平方加速。但是这些技术真的可以在实践中使用吗？

对于直接加速传统机器学习技术的大多数尝试而言，最持久的困难是要求技术能够有效地加载数据，然后由量子设备进行叠加查询。我们还不知道如何构建这样的 QRAM（量子 RAM）技术。

Google 和麻省理工学院 (MIT) 最近发表了一份研究报告，明确地展示了“宽和深”神经网络如何在训练中实现指数级加速。具体来说，这利用了深度学习中的神经切线核模型。这项工作展示了如何解决 QML 通常面临的四个“读出细则”异议中的三个。然而，我们仍然不知道如何构建 QRAM 硬件。

QC Ware 的专利数据加载器协议是一个值得注意的工具，它试图减少（如果不能克服的话）QRAM 瓶颈。

QC Ware 在 11 量子比特 IonQ 量子设备上进行了数据加载器技术的概念演示，以实现流行的机器学习原语、最近质心分类器。

2) 更多计算空间

与其“渴望 QRAM 奇迹”，Mattias Troyer（微软）鼓励该领域搁置“大数据”问题，而专注于“小数据、大计算”问题。这类问题寻求从大的计算工作空间中获益。这是量子计算机能够提供的独一无二的东西（由于量子比特系统巨大的希尔伯特空间）。

Xanadu 指出，对于近期的 QML 方法，许多最有前途的技术实际上最好理解为传统机器学习中的所谓的核方法。

IBM 声称 2021 年是一个显著的里程碑，它提供了一个学习任务示例，该任务可以提供指数级加速，但只需要对数据进行经典访问（尽管它确实需要 FTQC）。这将构建的一系列数据集作为起点，因此很难用传统算法进行分类（它们基于离散对数问题）。量子计算用作传统支持向量机的核函数。

IBM 还发表了量化 QNN（量子神经网络）与可比较的经典神经网络相比可以实现的更高维度的工作，以及难以模拟的经典特征图在影响可训练性方面的作用。

Pasqal 发布了一个专门定制的框架，以利用中性原子设备的可重构性来表示图的核。

非线性微分方程组是一类突出的问题，它们可以被简洁地表达，但是需要大量的计算资源来数值求解。这种方程出现在各种各样的科学和商业应用中，我们需要对复杂的过程进行建模：从结构工程到航空航天，从化学到生物学，从金融到流行病学。

Qu & Co 开发了一种新技术，用于处理近期量子计算机上的非线性微分方程，即可微量子电路。这种方法训练 QNN 以使用大的可用希尔伯特空间来处理导数。Qu & Co 还将这种方法扩展到随机微分方程。Qu & Co 已提交了一项涵盖其技术的专利申请。

自从现代计算的概念提出以来，自然语言处理就是一个值得关注的领域，也是近年来取得显著进展的一个领域。这是一个需要呈指数级增长的工作空间的问题的一个很好的例子（想想为什么我们有单词词典而不是句子词典）。

剑桥量子已经将 QNLP（量子自然语言处理）确定为 QML 的一个特殊领域。2021 年，他们报告了第一个实验结果。使用 5Q 的 IBM 设备对包含 130 个句子和 105 个名词短语的数据集进行编码。

QNLP 利用了量子计算机提供的扩展计算空间。剑桥量子提出的形式主义和量子力学的 ZX 微积分表示之间惊人的相似之处，这将是一个富有成效的方法。或许，正如剑桥量子力学的首席科学家 Bob Coecke 所说的那样，“语言是量子原生的”。

3) 独特的量子数据

一个越来越重要的关注点是，当数据集中存在需要解决的量子关联或量子干涉效应时，QML 应该能够超越经典机器学习。2021 年的工作已经开始将其形式化和结构化，这既适用于学习任务，也适用于生成模型。

加州理工学院在 2021 年发表了一项研究，对不同机器学习模型的能力进行

了界定：一种是传统的学习驱动，但使用量子系统的测量输出（例如，物理实验、模拟量子模拟器或 VQA 的迭代），另一种是在学习过程中保持量子相干性（未来的技术，可能有一天由 FTQC 实现）。一个关键的结果是经典驱动的 ML 可以做得很好，在“平均情况”预测精度方面与完全量子学习的能力相当。完全量子学习为“最坏情况”的预测准确性提供了进一步的指数优势。

Google 认为，支持量子可以为化学等领域的进步提供的最普遍的支持形式不仅是对系统的理论模拟，还可能包括为经典驱动的机器学习生成量子数据集。

量子电路玻恩机（QCBM）是一种实现生成模型的 VQA。2021 年发表的研究首次证明，一种特定类型的 QCBM，即伊辛玻恩机，可以执行任何经典计算机都难以完成的采样任务。

我们期望找到包含量子相关性的数据的一个地方是量子传感器的输出。在量子技术领域的其他领域，许多新的量子传感器正在积极开发中。然而，我们有时会忘记基于 NMR（核磁共振）和 SQUID（超导量子干涉装置）的设备已经使用多年（在医疗应用中，NMR 被称为 MRI）。

从实验中学习的量子优势——加州理工学院和 Google 的工作已经证明，在学习量子态的性质方面有指数优势。这项工作要求我们从两个方面来考虑“悬铃木”处理器。在第一种理论中，它的量子比特代表了某些假想物理实验的输出（或一系列量子传感器的输出）。我们的任务是了解这种状态的一些性质（研究物理或实验，或读出我们的传感器网络）。量子处理器的其余部分对这些输入执行纠缠操作，然后将输出传递给经典的机器学习程序。与纯粹的经典方法相比，这种方法能够以指数级的速度在更少的试验中了解状态的属性。

Google 发了一种用于核磁共振实验中检测到的量子辅助学习和系统表征算法。他们提出了 NISQ 和 FTQC 应用的资源估算。

Qu & Co 还提议将其 DQC 技术扩展到模型发现，我们希望找到支撑输入数据的微分方程。

在最冒险的情况下，有些人推测意识与量子波函数坍缩之间存在联系。事实

上,“客观坍缩”理论长期以来一直被视为扩展量子力学的一种可能方式。Hartmut Neven (Google 量子 AI 的负责人) 推测,波函数坍缩可能是一种有用的方式来理解我们将越来越需要分配给高级 AI 系统的“代理”。也许更多的人将不得不开始注意这种想法。

三、早期容错机器

1、平方加速还不够?

一个经典的与非门可能是每秒 10^{-9} 个晶体管,一个量子与非门(粗略地说)是每秒 10 个量子比特。这个巨大的 10^{10} 因子是仅提供适度的二次加速的算法的主要障碍。问题是,为了达到量子计算机获得优势的问题规模,我们已经在处理这样的情况:在完全 FTQC 的情况下,运行时间将是不切实际的长。

FTQC——早期设备经常讨论的标准规格是 100 万物理量子比特,2Q 保真度为 99.9%,以最近邻连接和 1MHz 的代码周期时间运行表面码。在这种潜在错误水平下,这可能是一台 1000 逻辑量子比特的机器。然而,量子优势的关键门(例如 T 门或 Toffoli 门)非常慢,每个都需要数百个逻辑量子比特。与传统计算机相比,这导致了巨大的“常数因子减速”。

那么其他的量子比特架构呢?它们提供了不同的门速度、相干时间保真度和量子比特连通性。2021 年的一项有趣的工作研究了这些不同的权衡对离子阱架构的影响。在当前的方法中,代码周期时间通常会更长,尽管这些架构的支持者认为,它们更强的扩展能力抵消了这一缺点。但这不能解决常数因子减速的基本问题。

PsiQuantum 提出了一种名为 FBQC 的新架构。光子时钟的时间可能非常快。然而,这些设备仍然会受到纠错解码所需的经典处理时间的限制。我们还不知道他们的逻辑时钟时间会是多少。

振幅放大 (Grover 搜索中使用的) 是一种量子原语,在商业优化问题中具有

广泛的潜在适用性，但它只提供平方加速。量子行走（或量子漫步）给出了一些例子，其中指数加速是可能的，但具有最明显的广泛业务利益的情况（例如加速蒙特卡罗模拟）只提供平方收益。这似乎是在开发现有的已知架构的基础上，将大量的商业应用转移到 FTQC 无法触及的范围之外。

D-Wave 在 NISQ 和 FTQC 早期都将量子退火作为其首选优化方法。另一方面，它宣布将构建哈密顿量模拟应用的门模型设备。

然而，随着该领域探索克服这一挑战的方法，我们也看到了创新。

Peter Johnson（Zapata 的首席研究科学家和联合创始人）评论道：“在早期容错量子计算时代，我们需要通过设计鲁棒量子算法来最大化这些机器的性能。这种算法仍将导致不可忽略的错误，但将减轻其对计算输出的影响”。这种方法可以让我们解决那些用 NISQ 错误率无法解决的问题，但却需要在 FTQC 的全面规模上花费一定的成本。Johnson 指出，最近这个领域的工作显示了这种方法的前进方向。

Iordanis Kerenidis（QC Ware 的国际量子算法负责人）指出，尽管一些我们之前认为具有指数优势的算法已经被经典方法的后续进展“反量化”了，但在实践中，它们在许多线性代数应用中仍然具有四次方或更好的优势。Kerenidis 著名的推荐系统仍然具有 8 次方的优势。

2、AlphaFold 与蛋白质折叠

蛋白质可能是最重要的生物分子。它们的物理形状及其如何影响它们之间的相互作用对生物功能和药物靶向有着深远的影响，所以这是一个备受研究重视的问题。解决蛋白质折叠问题一直是量子计算的潜在目标。

莱文塔尔悖论——一种短蛋白质可能很容易有 3198 种可能的键角组合。然而，一旦它形成一条长链，它就会在毫秒内采用一种独特的首选折叠形状。但是仅仅是依次尝试每一种组合所花费的时间就超过了整个宇宙的寿命！

这是蛋白质折叠问题，或者更准确地说，是一系列相关问题的集合，包括：

如何从氨基酸序列中预测简单蛋白质的结构；了解蛋白质构象；了解折叠的动态路径。

从量子力学的角度来看，不存在悖论，这只是一个经典计算难以解决但量子计算机可以解决的问题。

对于持怀疑态度的观察者来说，2021 年已经看到了对大肆宣传的量子预期的一些负面迹象。Google 旗下 DeepMind 开发的 AlphaFold 使用传统的人工智能方法来“解决”蛋白质折叠问题。制药行业还表明，当行业得到适当关注时，药物开发时间表可以大大加快。

AlphaFold 2 成功地将预测蛋白质折叠结构的最新技术提高到 92.4-95% GDT。对于单个蛋白质链，它在 90% 以上的时间里都能以合理的准确度 ($<3-4 \text{ \AA}$) 进行预测。这是一个戏剧性的结果，也是 DeepMind 迄今为止最引人注目的成功。甚至有人认为这是人工智能领域迄今为止最重要的成果。

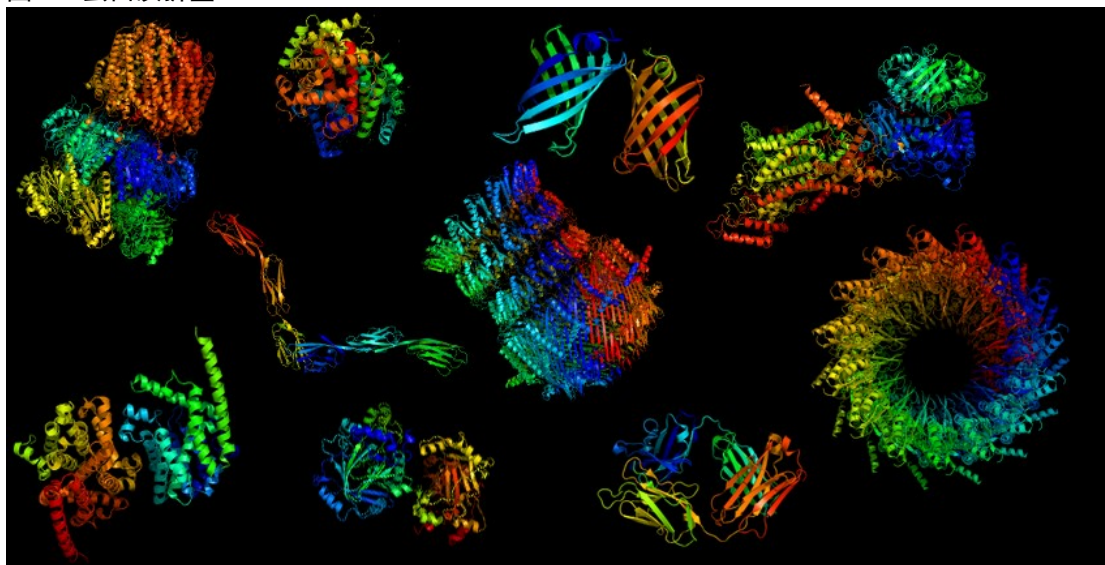
Bhushan Bonde 博士在 Quantum.Tech 2021 上的演讲，揭开了炒作和现实的面纱。传统的量子化学近似技术是筛选新冠肺炎 (Covid-19) 药物化合物的关键工具。但是，它们消耗了大量且不切实际的计算资源。他的模拟经常使用微软 Azure 云上的所有 GPU 能力；运行了数周，但仍然不够快。重复这样的实验会对能源消耗、热管理（冷却计算机硬件）以及更重要的时间效率产生影响。他还认为 AlphaFold 的表现还没有真正与制药公司的生物学相关，因为制药公司需要准确确认药物结合袋的准确性。

Bonde 博士认为未来的人工智能进步和量子计算技术是互补工具。量子计算为量子化学中的解析解提供了一个全新的工具。它还有望成为未来机器学习系统进一步提高性能的推动者之一，特别是当数据中存在量子相关性时。Bonde 博士认为，如果我们在生物系统中发现这些，我们不应该感到惊讶——我们关于鸟类导航能力的主要理论是基于鸟类眼睛中的感光隐花色素蛋白利用量子纠缠效应的能力。

IBM 一直积极推进量子蛋白质折叠方法，提出了一种量子资源高效的 VQE

变体，已经用于在他们的早期设备上“折叠”玩具问题。

图 17 蛋白质折叠



3、哈密顿量模拟和 FeMoco

哈密顿量模拟，模拟物理、材料科学或化学中的一般量子系统，从一开始就一直是量子计算的一个关键用例。每年，先进材料和化学品行业花费超过 400 亿美元用于测试潜在工业用途的新材料，大型制药公司花费超过 2100 亿美元用于研发。量子理论的支持者指出，通过提高研发管道的生产率和减少浪费在失败的临床试验上的资金，可以节省大量开支。

头条新闻经常会报道量子计算硬件的进展。算法也取得了巨大的进步，但是这一点并没有得到广泛的理解。模拟 FeMoco 一直是早期量子模拟领域希望达到的目标。

FeMoco ($\text{Fe}_7\text{MoS}_9\text{C}$) 是固氮酶中的活性位点，在自然界中负责将氮气催化转化为氨（肥料）。由于我们不明白蓝细菌是如何做到这一点的，所以我们使用能源密集型的哈伯-博施工艺来制造世界农业所依赖的肥料。然而，哈伯-博施工艺对环境的影响是所有化学工业工艺中最严重的。据估计，它所产生的二氧化碳排放量占全球排放总量的 1.2%，高于英国或法国！

模拟 FeMoco 所需的量子资源的详细工作为了解算法进展提供了一个窗口：所需资源的预测从 1 亿量子比特（2014 年）到 2000 万量子比特（2017 年）到 400 万量子比特（2020 年），再到今天的 200 万量子比特。对于 30 万至 100 万量子比特，还提出了较低分辨率的模拟。这一进展使得这种模拟在早期的 FTQC 机器上看起来触手可及。在研究这个问题多年后，Ryan Babbush（Google 的量子算法负责人）认为这些结果现在看起来接近最优，至少在当前的模拟方法和提议的纠错架构下是如此。

Schrödinger 和 Qu & Co 质疑，模拟 FeMoco 达到目前设想的精度水平是否足够。然而，他们也指出，有迹象表明，其他感兴趣的系统可能用比想象的更少的资源就可以解决。他们指出，Cr2 本身并不是一个具有实际意义的系统，而是一个潜在的交叉点，在这个交叉点上，量子优势将成为可能。

Babbush 热切希望在推动更高效的量子模拟方面开辟一条新战线，他评论说：“化学的未来是一次量子化的！”

与早期哈密顿量模拟（以及传统计算化学）中更常用的二次量子化方案相比，Babbush 提出了一次量子化实施的新方案，并完成了纠错计算的详细资源估计。这些方案提供了与二次量子化相似的准确性，但可以显著减少资源需求。

一次量子化——需要量子比特 $\propto$ 活性粒子数和 $\log$ （轨道数）

二次量子化——所需量子比特 $\propto$ 轨道数

这种形式主义的另一个优势是，它有望超越玻恩-奥本海默近似（将原子核视为经典点电荷）。

嗅觉和味觉——同位素是指只有同位素组成不同的分子。这种差异不会影响它们的化学性质，但有许多例子表明，这种变化会影响味觉和嗅觉的性质。这是量子隧穿辅助效应吗？

总的来说，谷歌看到了哪些 FTQC 用例？就物理量子比特而言，这些可能是：

- 2.5 万至 5 万量子比特——模拟快速加扰（通过 FTQC）。在理论物理中的潜在应用，在其他领域更有推测性。

- 5 万至 25 万量子比特——模拟晶格自旋模型。在核磁共振波谱分析中的潜在应用。
- 25 万至 100 万量子比特——以低分辨率模拟材料和分子
- 100 万至 500 万量子比特——以高分辨率模拟材料和分子

四、长远眼光

1、量子算法的大统一理论

潜在的商业用户经常会问，有多少种量子算法？从某种意义上说，学术团队和越来越多的初创公司每周都会发布新的算法。然而，新技术通常利用的底层原语数量要少得多。

哈密顿量模拟直接用于材料科学和化学；它也是 HHL 和连续时间量子行走的核心。QFT（量子傅里叶变换）用于相位估计、Shor 算法、求解离散对数问题等。振幅放大用于 Grover 搜索算法、离散时间量子行走和其他算法。

QuSoft、微软和麻省理工学院的新研究以一种新的方式看待量子算法。这个“量子算法的大统一理论”指出量子奇异值变换（QSVT）是几乎所有已知量子算法的统一基础原语。这种新的形式有望让人们深入了解量子算法的本质，以及它们可以在哪些方面提供量子优势

QSVT——这个过程用一个酉矩阵（幺正矩阵）表示。物理学家熟悉特征值和特征向量在分析这类系统时所起的有用作用。奇异值分解是特征分解到非方阵的数学推广。这样的矩阵可以嵌入到一个更大的酉矩阵中。QSVT 技术可以对嵌入矩阵的奇异值应用一个函数。

物理学家们可能会说，QSVT 技术允许我们在量子计算机的量子原生酉结构中嵌入更一般的问题。数学家们可能会说，QSVT 明确了如何将更广泛的数学函数映射到物理设备上。

2、BQP（有界错误量子多项式时间）可轻松解决？

我们应该对量子计算的长期价值抱有多少乐观态度？值得回顾的是，我们没有证据表明量子计算机可以解决传统计算机无法解决的问题。我们知道如何使用它们来分解大数字，但我们不知道是否能找到一个更好的方法，让传统计算机来解决这个问题。我们所拥有的只是直觉。

对于一些问题，很容易看出这种直觉的来源。每当我们想要模拟一个最终依赖于量子力学的真实系统时，甚至在传统计算机上编码哈密顿问题都是非常困难的。物理学家的直觉告诉我们，解决这个问题并不容易。由于其对材料科学和化学的影响，这仍然具有特殊的重要性，认为，这一技术的长期后果仍然没有得到广泛的重视。

但是，对于更广泛的问题，我们的直觉应该是怎样的呢？这里我们需要关注计算复杂性理论。我们还没有任何绝对的证据来证明量子计算机能够有效解决的问题（BQP）超出了传统计算机（BPP）的能力。乐观地说，我们也不知道量子计算机能力的上限在哪里（我们只知道 $P \subseteq BPP \subseteq BQP \subseteq PP \subseteq P\#P \subseteq PSPACE \subseteq EXP$ ；我们甚至不知道重要的问题类别与这个列表相交于何处，如 NP 或它的泛化 PH）。

Oracle——计算复杂性理论家有他们自己产生直觉的方法。当他们不能绝对地证明一个结果时，他们经常使用“相对证明”来取得启发性的进展，这种证明探索了假设一个 oracle 是可用的结果，我们可以询问（查询）来提供必要的输入或解。然后，我们可以通过研究调用 oracle 的次数（问题的查询复杂性）来取得进展。

这样的技术并不总是指向正确的方向（我们现在知道 $IP = PSPACE$, $MIP = NEXP$, $MIP \int = RE$ ）。然而，这些相关证据一次又一次地被证明是推动进步的有用垫脚石。特别是量子信息理论家在发现 Shor 算法和 Grover 算法的过程中使用了这样的技术。我们应该认真对待这种直觉。

在 oracle 模型中, 我们可以证明量子计算机可以超越经典的有效可能 ($BPPO \neq BQPO$), Bernstein-Vazirani 和 Simon 算法做到了这一点。这种分离最近被进一步推进, 以表明存在一种相对于量子机器具有超越任何经典机器的能力的预言 ($BQPO \not\subseteq PHO$)。我们还知道这个问题, Forrelation, 说明了查询复杂度接近最大的加速。

在最近的工作中, Scott Aaronson (美国德克萨斯大学奥斯汀分校) 和他的学生扩展了这一理论, 证明了一系列新的结果。这包括对一个长期存在的问题的答案 (我们已经知道 $NPBPP \subseteq BPPNP$, 我们现在知道相对于一些 oracle $NPBQP \not\subseteq BQPNP$)。有趣的是, 这些相对化技术似乎表明, 经典复杂性类的潜在坍塌和分离对量子计算机能力的限制少得惊人 (例如, P vs NP 的量子版本和经典版本是不耦合的)。这可能会鼓励一种直觉, 即确实存在一些只有量子计算机才能解决的尚未完全定义的问题。正如 Aaronson 所说, BQP 表演“杂技”的空间仍然很大。

复杂性理论似乎仍然有很多东西可以提供。Aaronson 提出了一个与量子查询复杂性有关的关键开放问题清单, 以促进研究进展。

仅提供平方加速的算法要在目前设想的早期容错机器范围内带来好处, 面临着艰苦的斗争。这自然将重点放在寻找提供更大加速的算法上。

Aaronson-Ambainis 猜想 (未经证实但被广泛相信) 告诉我们强 (指数) 量子加速只发生在结构问题 (在数学意义上)。也许商业直觉在这里也有帮助。业务问题通常有很多结构 (在现实世界的意义上)。然而, 也许我们过于关注我们已经定义的传统问题类别, 而对这些新设备的功能自然而然地将我们带到何处的关注不够? 企业是否甚至没有认识到一些最大的挑战和机遇, 因为它们可以通过不同类型的数学来解决?

我们完全有理由相信量子计算的显著潜力。2021 年的进展应该加强而不是削弱我们支持这一点的直觉。

五、展望 2022

- 量子随机性——谁会为量子生成的随机数买单？
- 量子退火——D-Wave 客户会在常规生产中使用量子退火应用吗？
- VQE——我们会在 NISQ 设备上看到“超越经典”的演示吗？
- QAOA——我们能清楚地看到什么时候这可能会带来优势吗？
- 量子蒙特卡罗——进一步的创新能让它成功吗？
- 量子机器学习——注意在基础科学研究中的应用。
- DQC——我们会看到实际用例的具体资源估算吗？
- QNLP——对于这个令人兴奋的方法，我们可以期待什么样的路线图？
- 量子化学——一次量子化形式将提供什么新的可能性？
- 欧洲的增长势头——关注 Beite、JoS Quantum、Fermioniq 等初创公司的更多信息。
- 鲁棒量子算法——关注探索 NISQ 以外空间的进展，但不包括全尺寸 FTQC。
- NISQ 的其他架构——竞争性量子比特技术提供了不同的性能权衡。注意 NISQ 算法针对高连通性的离子阱平台进行调整。
- “适度”FTQC 的其他架构——需要注意评估高规格应用程序所需资源的工作。对于离子阱，理解更高的连通性与更慢的门速度的影响将是一个关键的考虑因素。
- 创新纠错——关注纠错的发展；量子 LDPC 码能引起轰动吗？
- 计算复杂性边界——永远记住，这个领域的正式基础是建立在一些大的猜想之上的，这些猜想对于事情的结果具有很大的灵活性。任何事态发展都可能对该行业产生重大影响：Aaronson-Ambainis 猜想；BQP vs NP 完全；BQP vs $NP \cap coNP$ ；甚至是 P vs NP 本身。
- 实验复杂性的前沿——记住，物理学家发明的每一个理论最终都会被推翻。量子力学也不会有什么不同。投资者希望每个新处理器都能工作。如果没有

的话，事情可能会更严重。

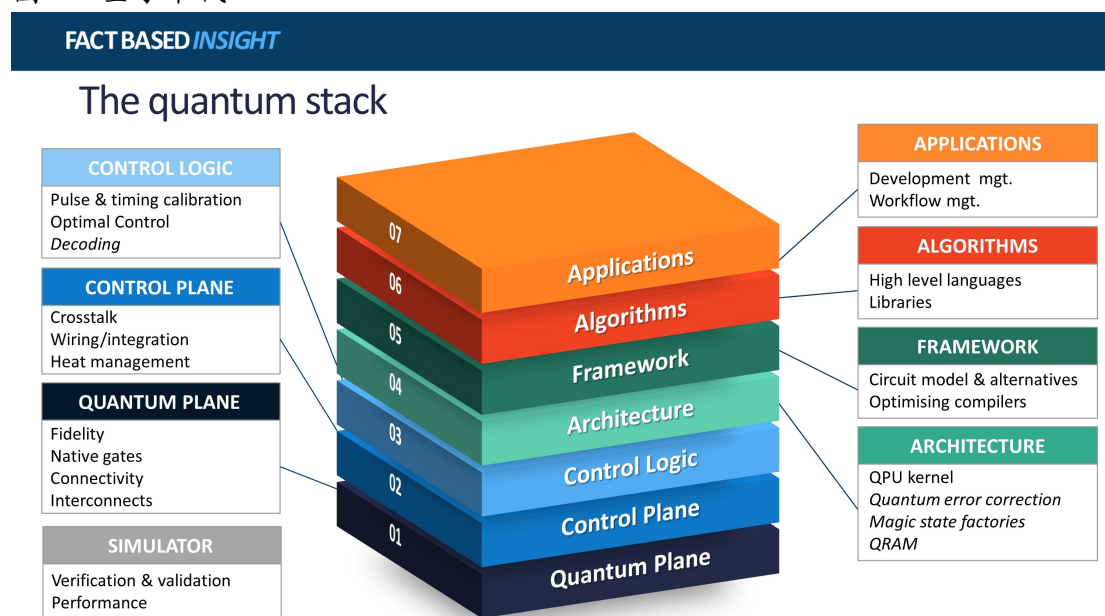
第三章 量子软件展望

IBM 继续引领量子云，但在服务早期量子应用方面面临真正的竞争。打造这个市场的未来看起来仍是一场持久战。选择一个有正确战略的合作伙伴可能比仅仅比较当今的产品功能更重要。

量子革命所依赖的远不止是构建一种新形式的计算硬件。创新的量子算法也同样重要，因此，让这些算法更容易开发和部署到实际的商业应用将是一个核心问题。

找到正确的框架将这些数学转化为程序形式也是关键，但门模型量子计算的电路和量子退火求解器并不是唯一的故事。纠错是量子故事的关键部分，也需要找到它的位置。在最底层，量子比特需要模拟控制，这本身就是一个充满挑战和机遇的接缝。量子堆栈中没有一层不值得我们密切关注。量子堆栈如下所示：

图 18 量子堆栈



应用程序——面向商业的最终用途应用程序。在很大程度上，这些工作仍在进行中。许多参与者强调早期研究和用户社区参与，以开发概念验证和试用应用程序。

算法——解决各类问题的独特量子方法，请参阅量子算法展望 2022。

框架——大多数早期参与者强调电路模型量子计算（尽管这种方法有重要的变化）。各种提供商提供了自己描述和执行所需量子电路的方式。

架构——协调计算操作的运行时环境。包括量子门、测量和紧密耦合的经典逻辑。最终，我们可以期待核得到优化，以高效地实现量子纠错，并协调对专业资源的访问，如魔法态（magic state）工厂和 QRAM。

控制——模拟脉冲驱动的低电平操作（通常基于微波或激光）。脉冲形状和时间至关重要，需要高级协议来优化门操作和抑制串扰。

量子——实际的量子比特硬件。请参阅量子硬件展望 2022。

模拟器——传统模拟器是软件堆栈中的一个关键附加元素，这不仅仅是因为当前量子处理器的性能有限，而且也是为了支持正在进行的程序开发和调试。

量子软件行业的发展正在迅速进行。然而，对量子硬件和量子算法进展的回顾表明，这可能仍然是一场漫长的游戏。对于早期采用量子的人和潜在的量子开发者来说，最重要的考虑可能不是立即可用的软件产品功能，而是选择正确的合作伙伴。要了解当前的市场状况，投资者必须了解早期参与者面临的挑战和机遇，以及他们正在发展的不同长期商业战略。

一、量子先驱

在量子软件的“萌芽”阶段，IBM 显然是早期的胜利者。虽然是其他人第一次将量子处理器应用到云上（2013 年布里斯托大学的 Jeremy O'Brien，现在他是 PsiQ 的创始人），但是真正成功推动参与度发生一步变化的是 2016 年 IBM Quantum Experience 的推出。现在更名为 IBM Quantum，拥有超过 36 万名注册用户，2021 年平均每天执行 22 亿次电路，通常任何时候都有 25 个量子处理器在线。

IBM Quantum Experience 最初专注于通过提供一个简单的图形化 web 界面允许用户创建（编写）简单的量子程序（电路），然后在早期的量子硬件上运行

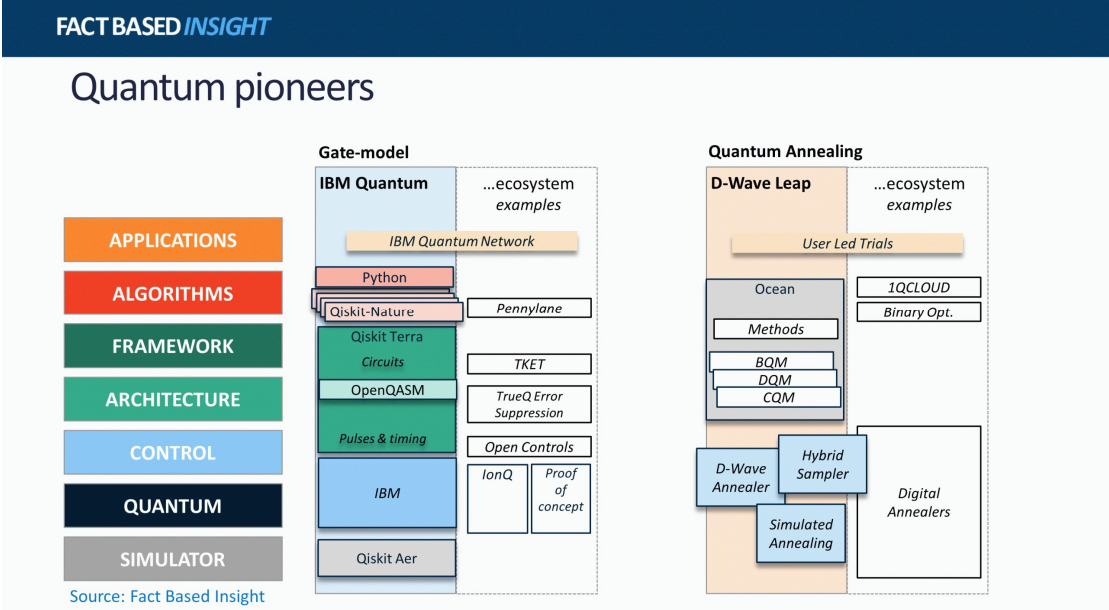
它们。IBM 在这一成功的基础上引入了 Qiskit，这是一种适合于科学和早期行业采用者使用的开源编程框架。与该方案一致的教育资源和活动一直是重点。它的 OpenQASM 底层电路表示语言已成为事实上的行业标准。OpenQASM 3.0 规范草案于 2021 年发布，并继续吸引跨行业的兴趣并支持。与 AQT 以及最近与 IonQ 的一系列概念验证展示了 Qiskit 对多种量子比特硬件类型的适用性。如今，IBM Quantum Network 的合作伙伴包括商业巨头戴姆勒、埃克森美孚、摩根大通、三星、高盛、埃森哲、波音和 LG 电子，总共有 130 多名成员。内部设施和战略合作伙伴包括弗劳恩霍夫（德国）、东京大学（日本）、克利夫兰诊所（医疗保健）和延世大学（韩国）。这与 IBM 的整体业务技术和服务产品齐头并进。

要真正理解 IBM 思想的战略方面，请回想一下，在狭义上，实际上并不需要这种全局硬件访问。广义地说，我们可以很容易地模拟 40Q 左右的量子处理器。IBM 正确地认识到，教育和更广泛的生态系统参与需要获得真正设备的兴奋。它还认识到，帮助人们学习量子基础知识将建立强大的商业势头。

D-Wave 在其早期战略方面也取得了重大成功。2011 年，D-Wave 首次推出商用量子计算机，关于其独特的硬件战略的争论至今仍在继续，尽管现在各方都普遍接受了其局限性和可能性。尽管如此，D-Wave 独特的、用户主导的试验方法的成功值得关注。虽然让应用进入日常的生产使用是很困难的，但我们相信客户已经看到了业务价值。企业需要激励他们最优秀和最聪明的人以新的方式思考他们的业务问题。收益通过多种方式返回到业务中。D-Wave 在为长期留住客户的战斗中不断创新。

D-Wave Leap 云和 Ocean 开发环境为面向商业的量子退火应用提供了平台。这套工具已经发展到包括混合量子退火/经典求解器。该服务的最新发展强调了算法工具的易用性，以及工作跟踪和可视化界面。对简单性和稳健性的关注是为支持生产应用程序而设计的。在坚持量子退火优化问题的同时，D-Wave 还宣布了建造门模型量子计算机的计划，以解决材料科学和量子化学模拟问题。

图 19 领先的量子公司



门模型量子计算界的一些人可能会试图将应用投入生产的延迟解释为某种程度上反映了量子退火的一个弱点。然而，换个角度来说，在没有纠错和大规模机器的情况下，早期门模型的成功也可能是渐进的，而不是革命性的。D-Wave的经验实际上提醒我们，在任何大型客户组织中实施变革是多么困难。专业服务部门早就明白这一点，并越来越愿意提供帮助。不应低估其未来作用的重要性。

二、早期门模型量子计算全栈公司

对于门模型量子计算中的许多早期硬件玩家来说，创建自己的完整软件堆栈只是一个必要的事情。然而，“全栈”并不意味着一个进化到 IBM 能够构建的程度的服务产品。

Google——在 2019 年展示了“量子霸权”之后，Google 围绕 Cirq 框架明确了其堆栈。2021 的一个值得注意的是 Stim，这是一款稳定器电路模拟器，其独特之处在于专注于支持量子纠错研究。

Rigetti Computing——在紧密的经典循环中率先执行量子电路。这种对 VQA 友好的技术最近才进入 IBM 运行时环境。Rigetti 现在跟随 IBM 的脚步，引入了

Quil-T (Quil 指令集架构的脉冲级扩展)，以开放对系统的控制。这是 Quil 的一个扩展，它允许 Rigetti 设备作为三能级系统，即 qutrit，而不仅仅是作为标准量子比特进行操作。

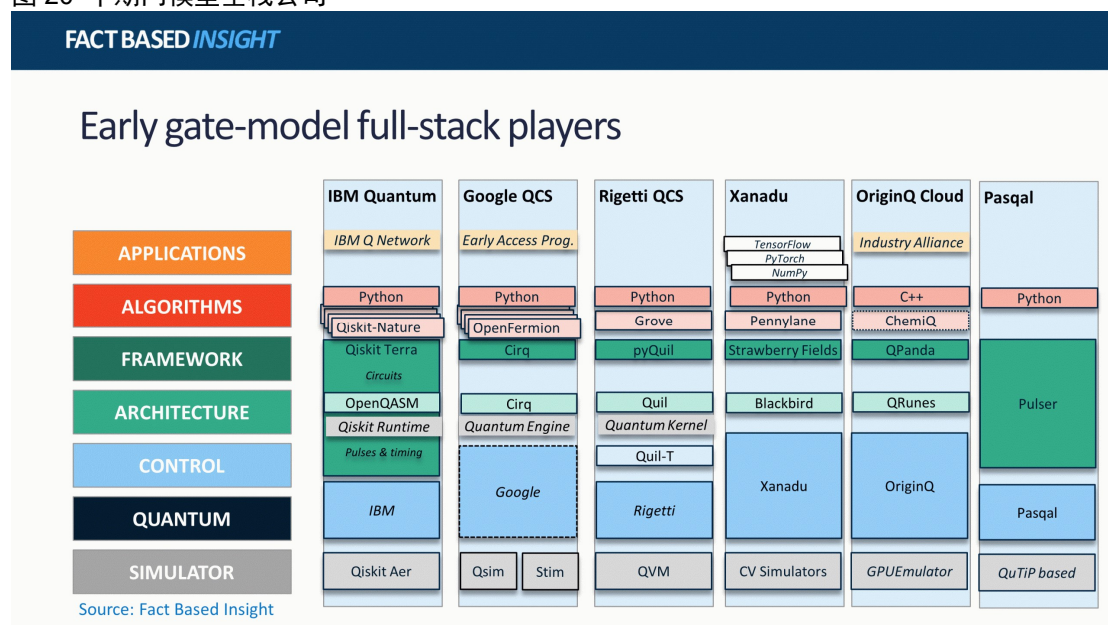
Xanadu——Strawberry Fields 框架支持 Xanadu 独特的光量子计算方法。此外，他们有影响力的算法库 PennyLane 与其他各种门模型机器兼容。

本源量子——中国量子计算的前驱。他们的堆栈已经在他们自主开发的超导和硅量子比特处理器上得到了验证。

稍晚加入的硬件玩家现在可以利用一个生态系统，让他们不必构建软件堆栈的上层。我们仍然可以期待进一步的创新，即玩家将寻找与他们的量子比特平台相关的特定机会。

Pasqal——引入脉冲发生器，以支持其设备的脉冲电平控制。由于中性原子器件在量子模拟中的潜在应用，这对中性原子器件具有双重意义。

图 20 早期门模型全栈公司

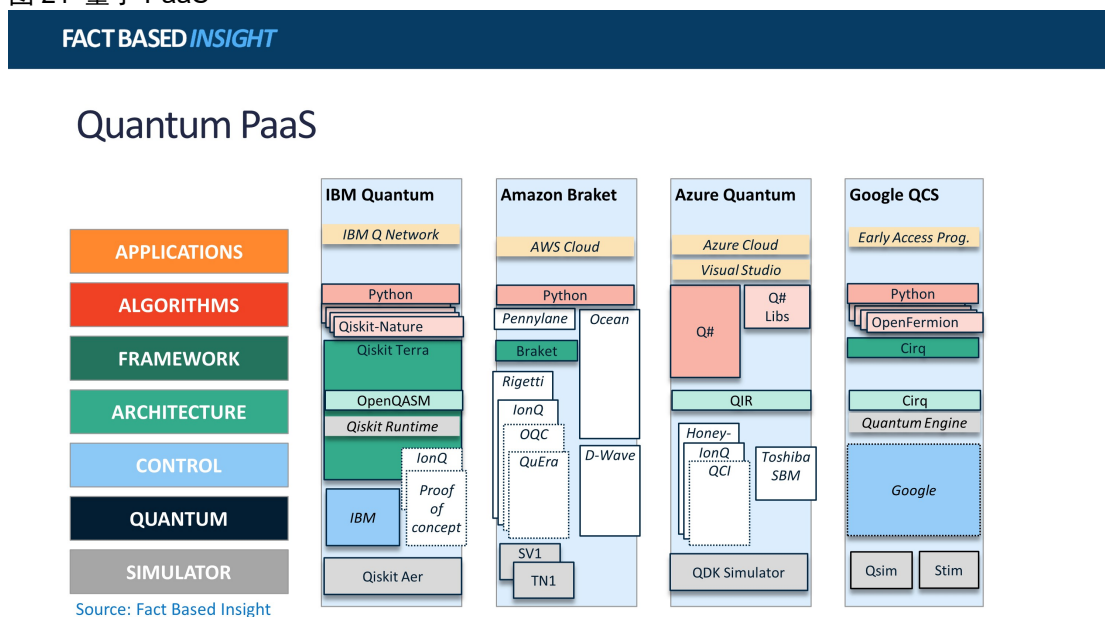


花时间公开披露、记录和支持堆栈的较低层会带来成本。这种精细特性可能会为供应商的本地生态系统带来额外的创新和性能。但是有多少最终用户将直接访问它们？策略师必须根据具体情况权衡成本和收益。

三、量子平台即服务

没有人真正知道什么样的量子硬件战略会胜出。因此，早期采用者通常会寻求一个最大程度上不依赖硬件的平台。这非常符合 PaaS（平台即服务）产品的概念。领先的传统云计算巨头 AWS 和微软 Azure 已经与 IBM 等开始争夺量子云市场。

图 21 量子 PaaS



IBM Quantum 一直强调它为自己的量子后端提供的访问权限。（Qiskit 支持访问其他提供商后端，但这些后端目前尚未完全集成到真正的 PaaS 产品中）。

IBM 在其处理器群中增加了 VQA 友好的 Qiskit 运行时容器（从 2022 年开始包括动态中间电路测量和前馈），这是 IBM 构建真正的“无服务器”云产品计划的第一步。这不仅需要与核紧密耦合的经典资源，还需要计算的实质部分可以卸载的资源。2021 年，IBM 完成了对电路编织和电路嵌入的概念论证（通过将部分计算部分卸载到经典资源中来减少所需的量子资源的技术），并演示了 IBM 云代码引擎如何将资源结合起来。量子无服务器模型的引入是 IBM 从 2023 年开始准备好支持真正应用程序（具有量子优势）部署的关键部分。

一名用户评论道：“IBM 花了大量的时间和金钱来完善基于 web 的终端用户前端，它提供了复杂的作业管理、排队和处理功能、数据存储、研究团队、资源认证和授权，所有这些都在一个处理 10 万用户的服务中。而其他供应商都无法达到这里提供的复杂程度。”随着硬件的成熟，IBM 似乎已经做好了充分的准备，利用他们的能力来服务大量的用户。其他供应商将需要努力完善他们的服务基础设施到这个程度。

亚马逊 Braket 已经开始在这个市场上提供 D-Wave、IonQ、Rigetti 和 OQC 设备的接入服务，QuEra 也将很快加入。对 PennyLane 的支持是另一个值得注意的特点。以及各种强大的模拟器。为了自主开发量子计算机，亚马逊在加州理工学院的 AWS 量子计算中心和亚马逊量子解决方案实验室进行投资并招募了大量专家。

一名用户评论道：“Braket 框架和电路 API 没有 Qiskit 提供的全面，在一定程度上限制了目前可以运行的应用程序的复杂性。”因此，亚马逊要想成功，就必须改善这一点。然而，几乎所有人都同意，量子计算将始终是计算的一种混合形式。通过 AWS 在更广泛的云市场的领导地位，Braket 很好地利用了对企业友好的供应灵活性。

微软 Azure Quantum 也在利用其母公司在更广泛的云计算领域的竞争地位。其 Azure Quantum 平台已正式公开。微软开发了 Q# 作为一种专门用于编写量子算法的语言，以及相关的库和培训资源。最近增加了还对 Qiskit 和 Cirq 框架中编写的代码的支持，承认了这些方法在更广泛的生态系统中的影响。微软通过其 Q Station 网络在量子研究方面有着悠久的历史。

或许，微软比其他主要玩家更倾向于将真正的量子优越性视为一场持久战。因此，在 Azure Quantum 中看到受量子启发的数字退火解决方案备受瞩目或许并不令人意外。

Braket 和 Azure Quantum 产品与 IBM 的不同之处在于，它们提供高级作业管理和服务工具，以补充越来越多的硬件供应商。

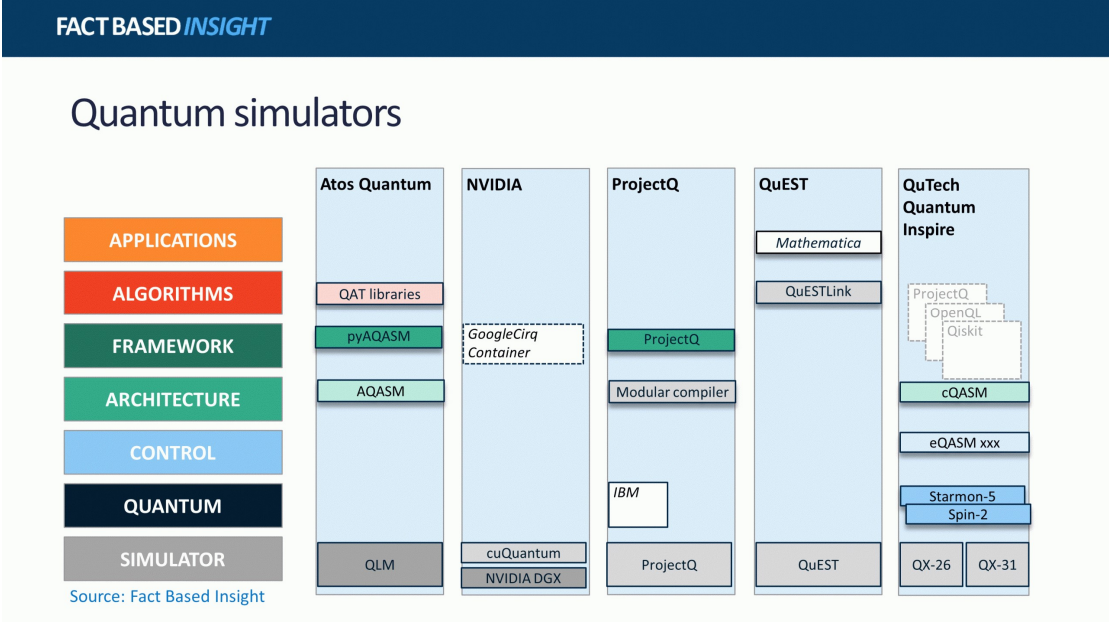
Google 在量子领域处于领先地位，在传统云计算领域排名第三。然而它的量子计算服务尚未越过早期访问计划阶段。这反映了公司将设备操作从“一次性科学实验”转移到常规生产服务所需的时间。它也不想推出一项仅基于仍可经典模拟的处理器服务。

值得一提的是，Xanadu 的 Borealis 是唯一云上提供的可以实现“量子计算优越性”的机器。

四、量子模拟器

传统的模拟器仍然是量子研发的有效并行途径。模拟通常可以达到大约 40 量子比特（如果我们能够简化，则可以更多）。高级模拟器甚至可以内置真实的噪声模型。无论如何，量子模拟器都可能在调试和验证量子应用程序中发挥关键的持续作用。

图 22 量子模拟器



QLM（量子学习机）——Atos 公司已经在其专用的量子模拟器硬件 QLM 上建立了一个完整的软件堆栈。这正在扩展到针对数字退火应用的量子启发算法的

执行。

学术项目——一些具有学术渊源的模拟器，如 ProjectQ 和 QuEST，为量子算法实验提供了自己的学术基础。模拟器也是 Quantum Inspire 平台产品的重要组成部分。

英伟达推出了 cuQuantum，以便在其基于 GPU 的硬件上进行快速量子模拟。2022 年早些时候，包括 cuQuantum 和 Google 的 Cirq 框架在内的容器将可用于英伟达 DGX 硬件，届时采用将变得更加容易。

两个著名的开源模拟器，阿里巴巴“太章”和华为 HiQsimulator 在 2021 年没有看到进一步的发展。然而，华为一直在积极支持 ProjectQ。

五、量子软件初创公司

也许最初的数字革命中最大的惊喜之一是由软件初创公司驱动的持续创新的重要性。在当前的量子革命中，我们看到全球范围内出现了一波量子软件创业浪潮，这并不令人惊讶。一个关键的问题是，在量子计算的广泛商业应用深入人心和更传统的市场发展起来之前，他们的战略是什么？对于管理层和投资者来说，一个至关重要的问题是，企业要运营多少年才能实现这一理想？

量子软件初创公司一直在追求各种策略。

1、寻求长期支持

一种策略是被另一家公司收购/合并，获得至少中期所需的资金支持。例如，实现量子硬件所需的资金规模，可以让软件开发活动看起来很便宜。从炙手可热的最终用途部门溢出的资金正在创造替代机会。

澳大利亚量子软件公司 QxBranch 可能是第一家采取这种做法的公司，他们在 2019 年被 Rigetti 收购。它的关系帮助 Rigetti 将其足迹扩展到美国以外。然而，软件和应用在 2021 年 Rigetti 的 SPAC 上市中并没有占据显著位置。

剑桥量子与霍尼韦尔分拆出来的量子解决方案部门的合并是另一项将硬件

和软件结合在一起的交易。然而，这里的策略似乎明显是为了保持与硬件无关的软件程序的势头。

英国量子软件公司 Rakho 最近被 Odyssey Therapeutics 收购，Odyssey 本身是一家新近成立的精密医学初创公司，专注于尖端药物发现方法。生物技术领域现有的巨额资金让这些公司能够选择自己想要开发的工具，作为自己长期发展的一部分。Odyssey 公司实际上拥有重要的量子算法能力。

Qu&Co 和 Pasqal 也宣布合并。Qu&Co 对现有的 NISQ 方法（如 VQE）能在多快的时间内达到真正的量子化学应用所需的精度持怀疑态度。同样，Pasqal 的中性原子硬件开辟了有趣的替代方案的可能性，如模拟量子模拟。Pasqal 将欢迎顶尖软件人才关注这个相对未开发的领域。

其他软件初创公司对其融资和成长历程有不同的看法。

2、从算法到应用

许多参与者面临的一个挑战是，如何将深度和高度专业化的量子算法专业知识构建成能够应用于各种潜在的现实世界应用的能力。一个重要的障碍是，业务洞察力是行业领域特定的，有时甚至是地理位置特定的，而且往往需要终生学习！

（1）扩大专有技术

一个关键战略是将算法智能与使能软件结合起来，并与潜在的最终用户一起应对识别和构建关键应用用例的挑战。最终目标是将学到的知识转化为最终可以产品化的服务。国家量子计划往往乐于提供帮助。面临的挑战是如何避免被拖入传统的咨询业务模式：稀缺的量子算法专业知识不容易扩展，传统咨询不能提供量子风险投资支持者通常寻求的回报。

一种常见的方法是提供量子机会评估和试点项目。理想的情况是看到这些公司发展成为与知名客户的大额客户关系。客户将从被视为活跃在重要的未来领域，以及从启动到他们自己的研发活动中受益。

QC Ware 有一个活跃的算法研究项目，并利用他们的 Forge 平台来支持高效

的项目执行，以及将专有技术打包到未来的服务产品中。值得注意的功能包括具有广泛适用性的组件，如数据加载器和低电路深度振幅估计。这些都被用于优化库、QML、线性代数库和蒙特卡罗模拟库。基于他们的混合动力优化方法，他们在 2021 年成功赢得了宝马量子计算挑战赛，并赢得了罗氏、勃林格殷格翰和科思创等著名客户。他们对行业领先的 Q2B 活动的长期推广已经证明是一个有远见的成功举措。

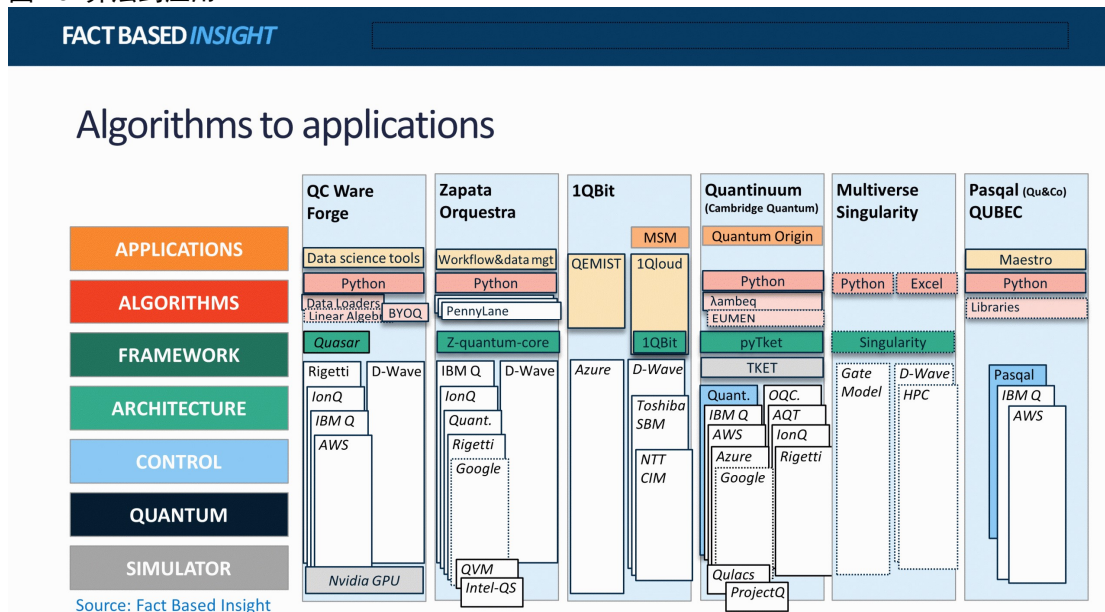
Zapata 也以其算法研究而闻名。其 Orchestra 平台针对的是工作流和数据管理问题，这些问题可能是部署应用程序时面临的常见挑战。Orchestra 提供创作和运营支持，并支持公共和私有云解决方案。客户包括化工、能源和食品饮料行业的前五大公司。我们认为，这一工具特别适合帮助客户将个人的专业知识转化为组织学习。

1Qbit 一直是量子服务领域的先驱，它通过利用其 1QCloud 优化平台建立了这一领域。1Qbit 率先强调量子启发的解决方案，将其作为提供给客户的一部分（现在其他公司也在效仿）。基于他们在优化方面的工作，1Qbit 在 2021 年取得了显著的成功，赢得了宝马量子计算挑战。

Quantinuum（前身为剑桥量子）利用其 TKET 编译器的领先性能及其所提供的跨硬件能力，在潜在的量子应用领域占有一席之地。它正利用这一势头，直接瞄准与主要商业和机构合作伙伴的长期合作关系。

软件即服务（SaaS）——Quantinuum 推出了 Quantum Origin 网络安全密钥生成解决方案。我们可以预期这项服务将发展到其他网络安全应用领域。像这样的服务能在多大程度上产生持续的收入增长，将是更广泛市场备受关注的焦点。

图 23 算法到应用



(2) 专注于专业知识

这种策略的一种变体是更具体地关注应用领域的专业知识。这样一种策略的好处是，可以磨练内部、行业特定的应用程序/算法技能，这可能是未来差异化的关键。在传统的软件世界中，这是一条很常见的道路。这也为量子启发的应用提供了一个更容易获得早期收益的途径。

Multiverse Computing 专注于金融服务。他们的 Singularity 工具包强调在安全意识强的银行环境中运行的能力，并提供量子启发和量子解决方案。同时提供 Python 和 Excel 前端集成，这是客户端工作流意识的一个标志。Multiverse 一直处于金融领域概念验证应用示范的最前沿。

Qu&Co 以量子化学为重点，开始了他们的发展。他们的 QUBEC 软件平台现在处于测试阶段。一个显著的特点是与 Schrödinger 公司领先的传统量子化学软件包的 Maestro 化学建模接口集成。Qu&Co 也有能力扩大这一基础，最近凭借其开创性的偏微分方程量子算法赢得了宝马量子计算挑战。目前 Qu&Co 已被 Pasqal 收购。

Phasecraft 专注于材料科学，将其作为量子优势最快实现的领域。其重点是

在 NISQ 设备上以有用的规模运行算法的基本智能（必要时达到脉冲级）。这并不是说该团队没有能力解决其他问题。只是他们认为首先解决这个问题是现实的。他们正受益于 UKRI（英国研究与创新）为电池材料设计项目提供的资金。

(3) 打包算法

许多玩家正在将特定的经验构建到算法库中。为了推动采用，这些软件通常都是在开源的基础上开发的，但是它们仍然有望成为为其赞助商建立重要价值链影响力的一种方式。事实上，有两个突出的例子说明了如何利用该领域的活动来补充公司的长期战略。

Xanadu 的 PennyLane 是一个量子机器学习库，其影响力已经远远超出了其母公司自身硬件的范围。最初的构想是作为量子机器学习的工具，提供机器学习社区熟悉的 NumPy 接口。这种格式已被证明适用于支持多种 VQA，因此 PennyLane 也在其他潜在的 NISQ 应用领域（如量子化学）中得到了应用。这是一个很好的方法，可以应对任何威胁，即其母公司天生独特的软件堆栈可能会与更广泛的社区“分离”。

Quantinuum 的 Lambeq 致力于开发面向量子自然语言处理（QNLP）应用的量子开发者的新生态系统；量子计算在这个领域有着引人入胜的、相对来说尚未开发的潜力。就好比，当你可以和其他人一起进行水电项目时，为什么还要控制一个小池塘呢？

(4) 让改变发生

基础更广泛的咨询公司也将在这个市场上发挥重要作用。既有 Reply 等技术专家（赢得空客 2020 量子计算挑战赛），也有更广泛的参与者：埃森哲（也是宝马 QC 挑战赛的获胜者）、波士顿咨询公司、德勤和麦肯锡都非常积极地建立自己的量子业务。主流咨询公司在将新想法转化为商业变革方面有着丰富的经验。他们还拥有推动实际项目所需的行业技能和国内资源。

值得一提的是，IBM 也是商业服务领域的一个强有力的参与者。随着价值创造的重点在这一领域的建立，它正朝着 IBM 相对于其他科技巨头的优势领域

发展。IBM 已经推出量子加速器，开始利用这一点。

3、更好的量子工具

一个互补的策略是提供量子软件开发者自己想要在近期、中期和长期使用的工具。然而，软件界对开源工具有强烈的偏好。面临的挑战是如何设计一种与此相适应的商业模式。

（1）社区门户

一种选择是寻求提供比别处更好的平台体验。这与培养量子新手兴趣的机会，以及真正认真避免与任何单一云供应商锁定的参与者结合得很好。Strangeworks 在开发平台的战略上一直处于领先地位，但我们也看到了其他领域的活动。

Strangeworks QC 提供了一个硬件无关的开发前端，它是新手最容易建立和运行的。关键它还提供了对尖端工具的访问，例如 TKET 编译器和 IBM Qiskit 运行时。社区库功能是一个很好的学习工具（跨多个框架），它将吸引那些理解这种思维方式给传统软件带来的价值的人。

Strangeworks EQ（企业量子）将后端访问添加到各种各样（且不断增长）的量子后端列表中。最近宣布的 Quantinuum 的 Quantum Origin 服务的集成是一个自然的选择。

Qapitan 是一家新成立的公司，有着建立量子 API 市场的有趣计划。目前处于私人测试阶段，这为开发者提供了一条简单的途径来交付和商业化 SaaS 产品，同时允许最终用户在市场发展过程中对替代产品进行基准测试和升级。

这类企业面临的一个中期挑战是，在客户更好地了解自己的需求和市场成熟之后，如何避免客户转移到其他地方，并使服务非中介化。这些平台将需要专注于它们所创造的真正可持续价值。

（2）扩展算法创作

一些公司正在瞄准解决量子算法设计挑战的工具。目前已知只有三种量子原语可以提供量子加速。然而，这些可以组合成算法来解决各种问题类。这些需要

进一步调整，以便在更广泛的业务应用中使用。为了解决实际感兴趣的问题，这些算法最终需要在很多很多量子比特的规模上实现。大多数专家设想，量子优势至少需要 100 个量子比特（要么是保真度比现在高得多的物理量子比特，要么是应用量子纠错后的逻辑量子比特）。

Classiq 试图在为具有更大数量量子比特的设备设计量子电路的问题上走在前面。正如我们不在门层编程传统设备一样，Classiq 通过实现可重用的模块化块结构简化了这一过程。它的聪明之处在于，相对于系统范围的约束，它自动化了优化多个独立块的过程，并允许程序员进行关键的权衡（如总体量子比特数或电路深度）。输出代码兼容所有主流平台。当使用今天的小型设备时，这似乎是一个概念性的开销，但类似的东西在未来可能是必不可少的。Classiq 相信它的方法将使复杂的电路更容易调试和维护。这可能是一个关键的证据。

Horizon Quantum Computing 正在追求一个特别大胆的愿景。它的目的是让用户只需使用高级经典语言编写代码，然后就可以从传统或量子执行中获益，而无需任何量子计算方面的特殊知识。一个关键的观点是，加速的机会不仅来自抽象的问题类，还来自常见的程序结构，如循环和数组操作。总的来说，Horizon 设想了一个编译链，它可以在多个细节层次上解包。许多量子算法面临的挑战是如何有效地实现从加减到求幂等常见函数。Horizon 已经在这一领域展示了概念验证方面的改进。Horizon 的愿景是大多数用户希望社区到达的目的地。然而，全面实现其承诺需要实现 FTQC、QRAM 和更快的量子体系结构等技术。

高级创作解决方案面临的一个短期挑战是当今量子硬件的能力有限。领先于开发游戏并探索未来的资源需求是一种有效的策略，但是客户对真正的量子执行的时间线的期望将不得不被管理。

(3) 优化的低级编译

在堆栈的底层，优化量子编译器必须处理一系列额外的独特量子挑战（本门集映射、量子位放置和路由、电路优化、错误缓解）。从技术上讲，我们实际上经常谈论一个编译（transpiling）操作，因为编译器链的多个部分都在发挥各

自的作用。

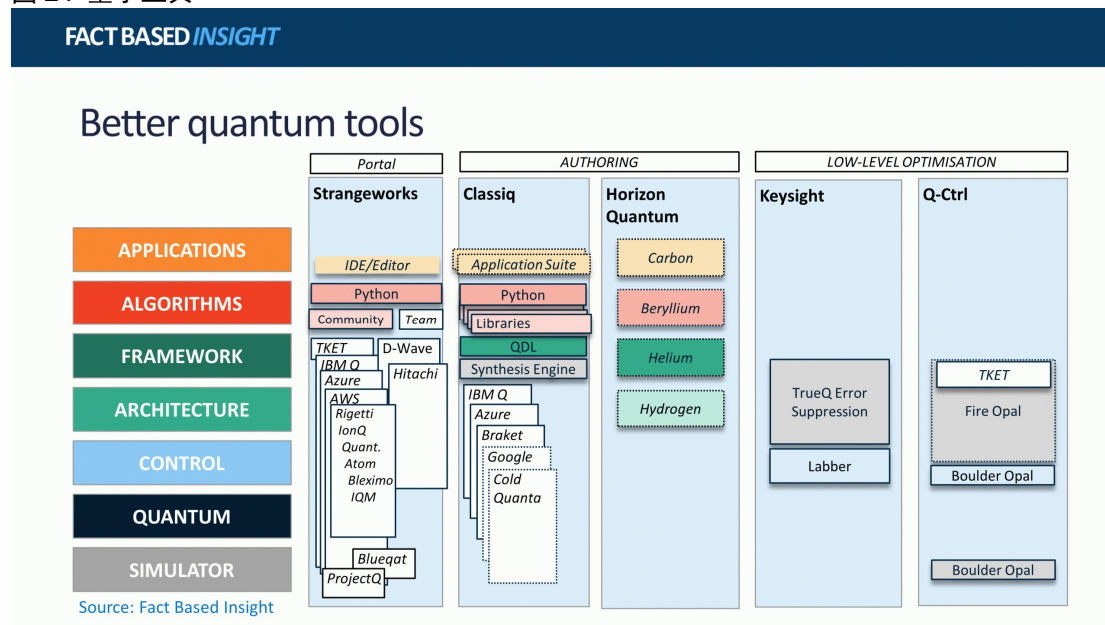
三个独立的低级量子编译器脱颖而出。每一个都展示了在这个市场上取得成功所必需的专有技术的独特方面。

TKET——这款旗舰版 NISQ 编译器能够在各种独特的量子框架之间高效传输，从而提供无与伦比的跨硬件能力。它为量子比特的放置和路由提供了有效的启发式方法。制作一个成功的量子优化编译器有一个强大的数学维度，在 TKET 的例子中，它利用了量子力学 ZX 演算公式中的概念。最近，Qermit 模块的添加简化了对常见错误缓解协议的支持。TKET 已被广泛用于各种前沿研究工作。TKET 现在是开源的，Quantinuum 希望在量子生态系统的核心建立自己的角色。

True-Q——Quantum Benchmark 公司在描述和缓解量子错误方面有着很强的传统。True-Q 采用随机编译技术，最初开发该技术是为了克服系统控制错误。现在，以多量子比特过程中的保真度为目标的周期基准测试技术增强了这一点。True-Q 在 2021 年的学术工作中因错误抑制和/或错误诊断获得了许多引用（包括谷歌 QAI、LBNL 的高级量子试验台、NASA、ORNL、NCSU，包括 Qiskit、Cirq 和 Quil 在内的各种框架，以及 AQT 的离子阱设备）。Quantum Benchmark 已于 2021 年被 Keysight Technologies（是德科技）收购。这是趋势的一部分，它将为量子堆栈提供一系列新的可能性。

Fire Opal——2022 年初向终端用户发布，这是低级编译器的新成员。它已经显示出令人印象深刻的初步成果。Q-Ctrl 在脉冲级“鲁棒”量子比特控制协议方面有着良好的记录。Fire Opal 作为一个物理门和脉冲级编译器，能够补充更高层级的优化编译器，如 TKET。2021 年，随着 Rigetti 和 Quantum Machines 加入 IBM，向第三方开放他们的硬件脉冲电平控制，市场已经转向 Q-Ctrl 的优势。Q-Ctrl 提供了与这些玩家的集成。它现在也在积极寻求利用其技术在量子传感应用。

图 24 量子工具



随着这一领域的不断发展,公开地比较编译器性能的能力将变得越来越重要。我们希望看到更多基准工作,例如编译器对 QV 和 CLOPS 的影响,以及整个 QED-C 基准测试套件。

在编译器领域,学术发展仍然非常重要。一个重要的主题是如何利用形式化方法的传统计算机科学技术。它们正在寻求一种数学上严格的方法来验证程序的正确性。在高度数学化但难以调试的量子电路编译世界中,这些技术可能比经典编程更有意义。

VOQC 的突出之处不仅在于其性能可与领先的编译器(如 Qiskit 或 Tket)媲美,还在于其电路优化在 Coq proof assistant 中被证明是正确的。

PyZX 是一款基于 ZX 演算的著名研究编译器。

六、建立低层控制

在传统计算中,门操作的低层控制早已转移到微体系结构和固件领域。然而,关键的挑战仍然存在于量子堆栈的这一层。量子比特从根本上说是模拟系统,它加剧了噪声和串扰的挑战,但也为智能优化控制和校准技术开辟了可能性。量子

纠错可能需要在扩展的代码补丁之间的紧密同步的读出和反馈。

一些参与者在专业控制电子领域拥有核心基础。这本身就是好东西。然而，我们需要明白，这些参与者中的许多人的雄心壮志并不仅仅停留在最底层。如果实现 NISQ 量子优势依赖于高度优化的低层性能，尤其是在这个将特定于应用的量子计算机推向前沿的世界中，这样的公司有望大放异彩。这可能会为他们创造一个获取更多价值的机会。

Quantum Machines 在为商业和学术量子计算工作提供控制系统方面有强大的全球影响力。该公司的量子编排平台（Quantum Orchestration Platform, QOP）专为规模化设计，并提供动态中间电路测量和前馈等重要功能。QOP 将经典和量子处理与 QUA 脉冲级语言和定制设计的脉冲处理器紧密结合，它将经典处理一直带到实时控制硬件。这是为了跨量子比特平台类型支持各种各样的量子用例而设计的。该公司认为，这种架构为 HPC 和云基础结构中异构量子计算的全面架构奠定了基础。

苏黎世仪器是一家成熟的科学仪器供应商。它的核心优势在于其硬件性能（尤其是锁定放大器）。目前它构建了一个完整的、专门的 QC 控制堆栈。这已经支持多种量子比特类型和低延迟测量反馈。苏黎世仪器最近被 Rohde&Schwarz 收购。它在量子控制中的强势地位是这一举措的关键部分，预计它将进一步加速这一进程。

Qblox 是从荷兰 QuTech 生态系统中衍生出来的公司（因此受益于多种量子比特硬件类型的直接体验）。它目前服务于 25 个学术和工业实验室。它提供了一个完全集成的控制和读出模块化解决方案，注重可扩展性。Qblox 赢得了瑞典查尔姆斯理工大学 20Q 解决方案的公开招标。核心优势在于其硬件（SYNQ 协议）的稳定性和时间同步性，以及低延迟反馈/控制流（LINQ 协议）。通过与另一家 QuTech 衍生公司 OrangeQS 合作，它在软件堆栈中的地位正在提升：它们共同维护开源的 Quantify 自动校准和表征软件。

随着 Keysight Technologies（是德科技）收购 Quantum Benchmark，将继续

加强其现有的量子产品套件——目前包括 Signadyne 的硬件和 Labber Quantum 的软件。我们预计，这些功能将结合到量子堆栈基础上的强大产品中。

除此之外，中国的中微达信、国盾量子、本源量子、国仪量子也是量子计算控制领域的核心参与者。

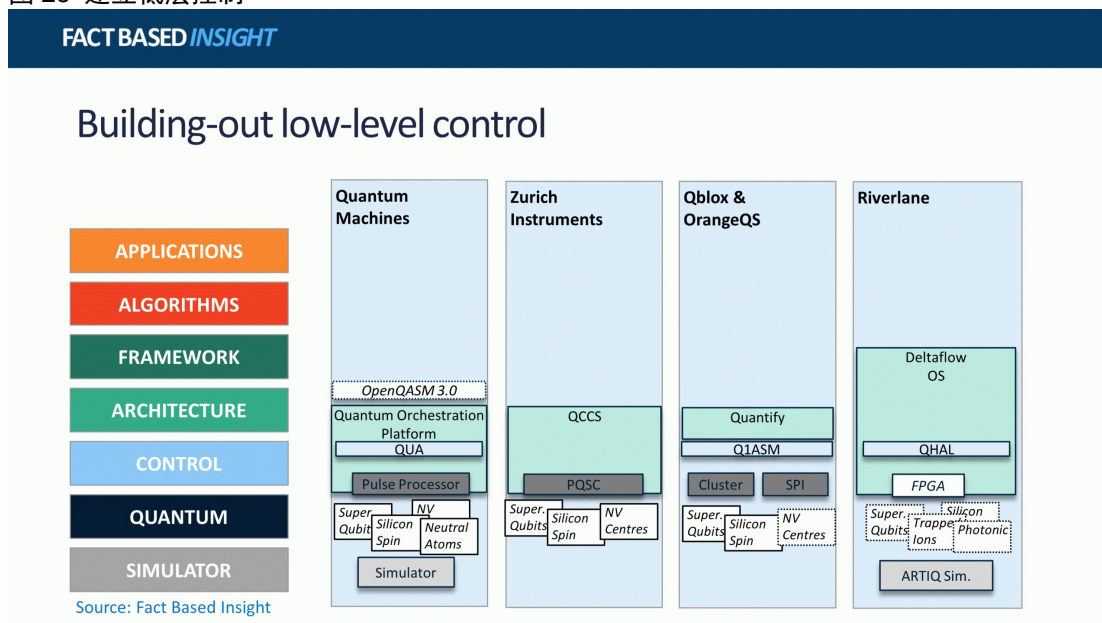
软件初创公司也被吸引到这一领域。

Riverlane 正在开发 Deltaflow.OS 量子计算操作系统，并获得由 UKRI 的拨款支持。这旨在为量子比特硬件开发者提供一个快速、可扩展的关键功能解决方案：低延迟、可扩展控制；自动校准和调整；在量子资源和经典资源之间协调运行时任务；纠错解码。这利用了分布式而非分层的节点网络。它已经用 Artiq（一种流行的离子阱控制系统）演示了试点集成。QHAL 硬件抽象层已经承诺兼容涉及四种量子比特技术的六种硬件。另一个由 UKRI 资助的项目 AutoQT 正在将机器学习领域的领先见解引入这项工作。

操作系统的一个问题是没有将量子堆栈的工作方式纳入一个模型中。它可以支持但确实需要传统的电路模型。它承诺将把最好的可用资源集中在困难的解码问题上，但它没有明确说明应该如何集成。

其他量子计算操作系统包括中国本源量子的本源司南、奥地利量子计算公司 ParityQC 的 ParityOS。

图 25 建立低层控制



在更广泛的背景下，OpenQASM 3.0（仍是一个“实时规范”）的定义明确地在之前架构层表达的门概念和经典控制概念以及通常在控制层表达的脉冲和定时概念之间建立了一座桥梁。量子栈将会进化。量子堆栈即将进化。

七、量子教育

IBM 早期成功的一个重要方面是它强调让 IBM Quantum 成为一个非常有用的教育工具。

Qiskit 和 IBM 量子挑战赛——Qiskit 教科书和教程资源被广泛认为是量子计算的重要入门资源。这些已经被成功的 IBM 量子系列挑战赛所补充。这些半辅导半竞赛的活动已经成为量子季的固定活动，对于有编程兴趣的个人来说，这是培养他们的量子技能的一个很好的方式。

Black Opal——Q-Ctrl 专注于量子比特的最佳控制。他们的内部可视化也是向量子新手教授量子比特和量子计算机的一种很好的方式。Black Opal 在线学习平台填补了市场上的巨大空白。它涵盖从波等基本物理原理，一直到使用自定义界面和电路可视化工具编程量子算法。Black Opal 对于量子新手来说是一个理想

的起点，即使他们计划通过更高级的特定于框架的课程继续进步。

Quantum Network Explorer——QuTech 之前进军教育领域的尝试是 Quantum Inspire。这继续提供了一个很好的学习环境，在一个已经由 IBM Quantum 主导的细分市场中追赶上来了。另一方面，它的 Quantum Network Explorer 将受益于率先进入更广阔的空间：如何通过网络处理量子比特。这引入了它自己的一系列新资源和概念，许多人认为这些资源和概念有朝一日将构成量子互联网的基础。

SpinQ（量旋科技）利用基于 NMR 量子比特的独特“桌面”量子计算机加速量子教育。2Q 双子座和 3Q 三角座使学生能够学习量子概念，并在真正的桌面设备上运行实验。量旋科技已经在他们的系统的基础上成功举办了一场高中量子计算竞赛，并为课堂提供了教材。接下来计划推出更紧凑的设备。

量子国际象棋——AWS 的 Aleksander Kubica 在 Q2B 量子国际象棋锦标赛上捍卫了自己的王冠，击败了来自 Zapata、D-Wave、Nvidia、谷歌、Quantinuum、Horizon 和 QC Ware 的对手。有时玩游戏是激发学生热情的最好方式。

教育是一种社会福利，同时也是一个很好的策略。它与那些有朝一日将推动量子革命向前发展的个人建立了密切的关系。这也为真正的收入机会打开了大门。

八、当前的研究主题——房间里的大象

目前，量子软件领域的许多实际焦点都集中在研究错误缓解技术上，这些技术旨在帮助我们在有限的 NISQ 设备上运行有用的算法。这些通常是增量的，在许多情况下，它们最终将无缝集成到堆栈中。然而，一些突出的挑战可能更具破坏性。

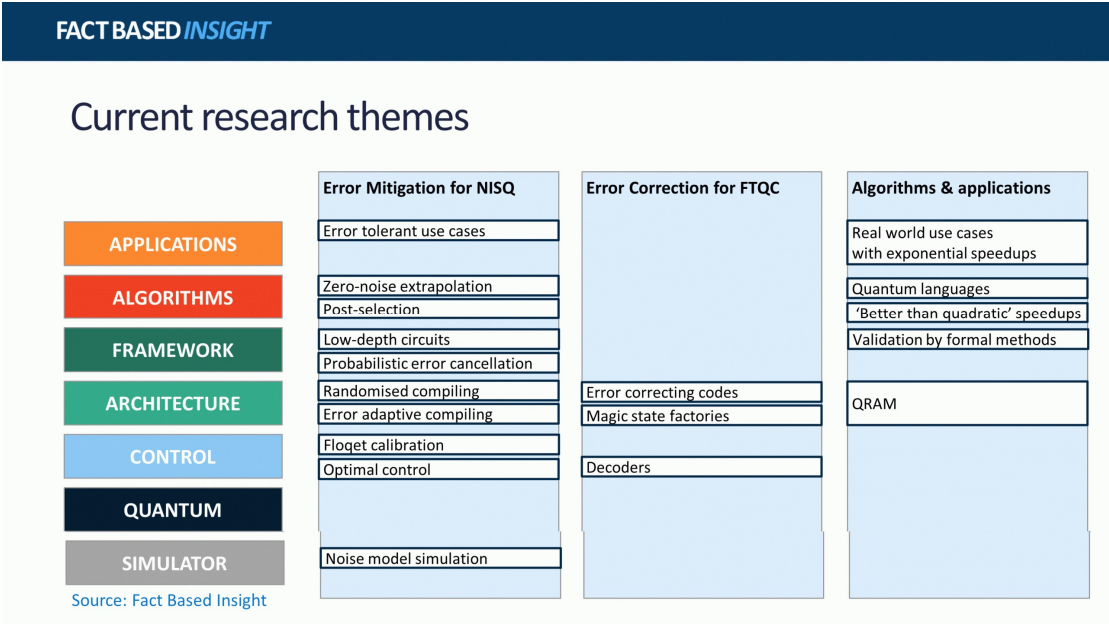
量子纠错是一个关键的量子计算概念，正迅速进入实用议程。对于许多硬件厂商来说，其开发是其硬件路线图的中心主题。越来越多的人指出，它不是一种全有或全无的开销，而是指它精心定制的应用程序如何通过量子优势线获得其他无法获得的算法。那么，为什么我们没有听到更多关于它在软件堆栈中的位置呢？

本报告的简化模型名义上将其置于架构层。然而，这不是既定的共识。一些从控制层建立起来的参与者会把它视为自己的自然领地。一些早期的算法参与者会希望密切监督它在早期应用中是如何使用的。对许多人来说，这里的数学将是一个挑战。

QEC 2021——正如纠错变得越来越实际，由于疫情的旅行限制，关于量子纠错的两年一度的前沿会议没有在 2021 年举行，希望我们不必等到 2023 年才能举行。

诸如线性时间联合查找解码器、改进的晶格手术协议、量子 LDPC 码和容错 3D 块等创新表明，这个领域仍然大有可为。

图 26 当前研究主题



用户最终不会关心量子纠错在哪里以及如何实现，只关心他们看到的量子比特是他们需要的质量。但量子堆栈的投资者现在需要关注这个问题。

我们很可能会面对这样一个世界：广泛的量子优势要求至少在某种程度上应用量子纠错。电路模型可以使物理量子比特和逻辑量子比特实现看起来非常相似。然而，这种转变可能会更加混乱。随着软件市场开始争论堆栈必须如何适应，预计会出现动荡。

九、展望 2022

- 超越经典——还没有可云访问的量子处理器展示“超越经典”的计算。2022 年这种情况会改变吗？
- 生产使用——哪个平台将率先在日常生产使用中托管量子应用？
- 中性原子——希望看到 Pasqal 软件团队探测这些系统的特殊能力，比如模拟量子模拟。ColdQuanta 的 Hilbert 云系统会鼓励其他人效仿吗？
- 光子学——既然 PsiQ 已经退出了隐身模式，我们会听到更多关于其 FBQC 将如何插入软件堆栈的信息吗？
- 云指标——只有 IBM 发布了有关其量子云使用情况的数据。其他人会效仿吗？注意竞争正在升温的迹象。
- 云基准——QED -C 在 2021 年产生了基于算法的优秀基准。我们会看到捕捉在量子云平台上运行的端到端体验的用户基准吗？
- 模拟器——如果你是认真的，你需要一个认真的模拟器。注意优化的模拟器性能，这是高端产品的一大优势。
- 商业模式——看看公司能否创造出适合自己的商业模式。很多人乐意做顾问，但谁能创造出专业知识呢？
- SaaS——Quantum Origin 等早期产品会引起什么兴趣？2022 年我们还会看到多少类似的服务？
- 编译器——注意特性、支持和开源策略的组合正在竞相推动编译器链的发展。标准度量和基准能够使性能对比更清晰吗？
- 量子 OS（操作系统）——低层控制系统能否进一步证明它们能够突破学术中心地带，成为商用量子计算机的真正独立操作系统？
- 参与和教育——IBM Quantum 在用户参与方面仍然保持着巨大的优势。我们会看到其他人正在迎头赶上的迹象吗？
- 量子国际象棋——Aleksander Kubica 是否会第三次蝉联量子象棋桂冠？我们

会看到 Quantum Chess 2.0 的商业版吗？

- 量子纠错——它在堆栈中的位置如何？

第四章 量子互联网展望

由于未来量子计算机带来的威胁，世界比以往任何时候都更需要更好的网络安全。大量新技术不断涌现，以满足用户的多样化需求。然而，要充分了解这一领域正在出现的竞争动态和政府行动，我们还必须了解长期的技术革命，许多人认为这场革命有朝一日将推动量子互联网的诞生。

我们的数字世界已经被许多黑客包围了。这些现有的威胁现在在一个完全不同的层面上又加入了一个。当一个足够大的量子计算机可用时，我们就知道它能够破解当前互联网和企业网络安全所依赖的公钥密码。更糟糕的是，今天截获和存储的数据已经很容易被这种未来的威胁解密。

世界范围内正在开展许多活动来应对这一威胁，包括新的基于数学的抗量子协议——后量子密码（PQC），以及基于物理的量子密码方法，尤其是量子密钥分发（QKD）和量子随机数发生器（QRNG）。新技术也为带外密钥传递的传统技术注入了活力。

然而，量子通信最终有望带来许多其他好处。一旦我们能够在远程位置之间可靠地共享量子纠缠，我们就知道如何利用它从根本上扩展量子计算机的能力并提供其他新功能。

与此同时，纳米卫星技术为网络安全解决方案和挑战打开新的视野。从长远来看，基于太空的分发有望加速纠缠网络的实现并模糊传统用例之间的区别。

要了解挑战和商业机会，我们必须了解这三个深度技术领域之间的相互作用——密码学、量子技术和太空。它们之间具有深远的协同作用的关系。

一、直接威胁

埃里克·施密特（前谷歌 CEO）说：“我强烈建议企业现在就应该采取行动。我们知道外国势力已经在忙着记录一切了，他们的计划是在 10 年后解密一切。”

Q-day（量子计算机可以破坏公钥加密的那一天）——Michele Mosca 和全球风险研究所发布了关于未来量子计算机何时能够威胁当前密码协议的最权威的专家意见调查。

当企业需要一个“合理的最坏情况”日期来做准备时，我们的建议是 2027 年，这建立在一个国家开展“曼哈顿式”项目的可能性之上。需要注意的是，更可能的日期是 2035 年或之后。

重要的是要认识到，这种威胁的规模和性质与我们通常面临的日常网络安全威胁完全不同。我们将可能面临的网络安全的系统性故障将是前所未有的。行业监管机构和保险承保人可能会越来越看不清未能做好准备的问题。

加密术语——完全部署的加密系统非常复杂。然而，简单地说，一个有用的高级模型有四个主要组成部分：熵、身份验证、密钥协议和消息加密：

表 1 不同加密技术的对比

案例	熵源	验证	密钥协议	消息加密
今天的互联网	Hash DBRG	RSA 2048	ECDH 256	AES 128
完全 PQC	CSPRNG	PQC 数字签名	PQC 密钥封装机制	对称
QRNG PQC	QRNG	PQC 数字签名	PQC 密钥封装机制	对称
带外传递	QRNG	带外	带外	对称
带内 QKD	QRNG	PQC DS	QKD	对称
ITS QKD	QRNG	PSK	QKD	OTP

二、后量子密码到达拐点

自 2006 年以来，一直在开发被认为能够抵抗量子攻击的基于数学的新加密协议，即后量子密码(PQC)。自 2016 年以来，美国国家标准与技术研究院(NIST)一直领导的一个项目，重点是标准化新的抗量子数字签名（PQC DS）和密钥封装机制（PQC KEM）协议。

NIST PQC 流程——第 1 轮评估了 69 个候选算法，其中 21 个被破坏或受到

严重攻击。第 2 轮有 26 个候选算法，其中 8 个遭受攻击。第三轮完成了 7 个入围算法的评估，其中一个遭受了重大打击。NIST 预计将在 2022 年宣布将使用哪些协议作为新标准的基础。草案将于 2022 年发布以征询公众意见，并于 2024 年定稿。

KEM/公钥加密决赛入围者：NTRU、CRYSTALS-KYBER、SABRE 和 Classic McEliece。其中，前三个是基于结构化格的方案，提供了良好安全性的同时拥有较高的性能，使其适合作为互联网安全性的替代方案。NIST 将最终标准化其中一种。Classic McEliece 有一个非常不同的配置文件，它提供非常短的密文长度，但是公钥非常长（262 KB）。重要的是，这是一种完全不同的基于代码的方案，已经经受住了 30 多年的攻击。

数字签名决赛入围者包括：FALCON、CRYSTALS-DILITHIUM、Rainbow。同样，前两个是基于结构化格的方案，NIST 将最终标准化其中一个。Rainbow 是一种多变量方案，虽然非常大的密钥大小使其不适合作为通用方案算法，但它增加了决赛算法的多样性。此前，比利时鲁汶大学（KU Leuven University）的工作降低了其安全性，迫使其作者调整他们的参数模型，Rainbow 遭受了又一次打击。

KEM 备选方案（5 个）：BIKE 是一种高效的基于结构化代码的方案，如果基于结构化格的方案失败，它则是互联网的潜在支持方案。HQC 是另一种基于代码的方案，其性能较差但可能具有更高的安全性。SIKE 是基于椭圆曲线同源的方案，拥有良好的带宽，但处理开销很高。NTRU Prime 是一种基于结构化格的方案，但它依赖于不同的结构假设（特别是避免解密失败）。FrodoKEM 是一种基于非结构化格的方案，性能受到很大影响，但提供了非常强大的安全承诺。

DS 备选方案：GeMSS 是另一种基于多变量的方案，也受到安全问题的影响。Picnic 是一种基于对称加密的方案，可提供更强的安全性。SPHINCS+ 是另一种对称的基于哈希的方案，可能提供最强的 PQC 签名。

根据 2022 年 7 月 5 日 NIST 公布名单，选择用于标准化的算法包括：用于

密钥建立的 CRYSTALS-KYBER，用于数字签名的 CRYSTALS-Dilithium、Falcon 和 SPHINCS+。此外，以下算法进入第四轮筛选：BIKE、Classic McEliece、HQC 和 SIKE。

虽然现在大多数人更喜欢干净利落地结束选择过程，但这对 NIST 来说仍然是一项艰难的权衡任务。

长期以来，结构化格加密一直被许多人视为 NIST 进程的主要竞争者。按照设计，它是安全性和性能之间的权衡。NIST 已经权衡了这些要求，选择的任何方案几乎肯定将构成未来常规安全部署的核心。

基于格的加密——于 1996 年首次推出，这一系列技术基于格上定义问题的计算难度。在其最强的实现中，安全性证明可以表明它们等价于最短向量问题的最坏情况困难。这简化为求解二面体群的隐藏子群问题，对于二面体群没有已知的有效的经典或量子攻击。

结构化的格——为了适应大多数常规部署（互联网和正常商业用途）的性能要求，密码学家通常建议使用“结构化”格。这牺牲了理论上的安全性以减少密钥大小并提高处理速度。

有一些知名人士表达了担忧。指出那些不熟悉 NIST 进程的人可能无法理解真正的风险权衡。

NTRU Prime 团队（NIST 进程中的一个备选协议）直言不讳：“NIST PQC 项目正在考虑的基于格的 KEM 比通常公认的要风险大得多”。该团队指出他们的方法（一种不同类型的结构化格）有着特定防御优势。

也有其他声音说 NTRU Prime 并不是中立的一方。但最重要的问题是 NIST 进程能够在多大程度上刺激真正的量子密码分析？大多数成功的攻击都是由于经典方法的创新（例如饱和、筛分、最小秩）。可以理解，这些是首先要解决的问题，但这也是对可能实现的目标的限制。

以及关于专利权的争论。

专利——法国国家科学研究中心 CRNS 继续声称，两个 NIST 结构化格决赛

方案 Kyber 和 SABRE 都属于其专利范围 (US 9094189B, EP 2537284)。Kyber 和 SABRE 团队 (他们自己都由法国领导/大力参与) 以数学为由对这一说法提出异议。然而, 问题不在于数学, 而在于未来的专利法院如何裁决, 这是一个法律问题而不是科学问题。

NIST 和 CRNS 之间为解决此问题而进行的谈判因成本问题而陷入停滞。一个不经意的商业观察者可能会期望一个简单的谈判解决方案。然而, 任何熟悉 PQC 论坛的人都会知道, 在加密社区中, 对这些问题的情绪高涨, 他们的绝大多数工作都是在这个过程中以无 IP 的方式提供的。有些人甚至争辩说, 向 CNRS 支付任何费用都将开创一个糟糕的先例, 特别是因为他们认为该专利不适用技术理由。具有讽刺意味的是, 在 NIST 进程中, 损失最多的是两个法国方案。一封由 60 名社区成员签名的信函已发送至 CRNS, 要求其改变立场。

最重要的是, 未来潜在诉讼的任何不确定性都将成为商业部署的一大障碍。一个更微妙的问题是, 如果 NIST 的最终选择被视为完全由非技术问题驱动, 则可能会削弱其在该领域中的支持。一些想法是标准化多个结构化格 KEM 方法。

对于 backdoors (后门) 的恐惧——很少有人认为 NIST 会故意批准带有后门或已知漏洞的协议。但是, 由于情报界 (美国国家安全局 NSA、GCHQ、DGSE 或其他机构) 操纵这个过程, 或者根本没有分享已知的秘密漏洞的知识, 那么就会导致批准带有后门或已知漏洞的协议被轻易被批准。尽管 NIST 已经大大加强了其流程, 但仍有许多人认为这在过去曾发生过。

Dustin Moody (NIST) 强调 “NIST 独立的做出决定, 并将 NSA 排除在我们的标准化过程之外。我们也会接受他们的意见, 就像我们接受任何重要利益相关者的意见一样。”

实际上, 所有参与这些争论的团体都相信格加密的巨大潜力。

1、问题类别的多样性很重要

寻求具有不同性能权衡的强大 PQC 的企业用户将不得不等待更长的时间来

等待更多 PQC 标准的出台。在 NIST 的 PQC 第 4 轮中对备选方案的持续评估将有助于弥补这一差距。

多样性非常重要，因为这仍然是一个正在发展中的领域。如果在一个协议或一系列协议中发现未来的弱点，我们需要准备好替代方案。

我们可以期望结构化格加密形成新一代互联网安全标准的基础。尽管早期存在担忧，但我们拥有可以以这种方式运作的协议，这是非常积极的。然而，应该指出的是，这种“最佳情况”的结果取决于一条相对狭窄的路径。

一个特别的担忧是，对于基于结构化格的数字签名方案，仍然没有通用的互联网兼容替代方案。这代表了新型量子攻击或常规攻击的潜在单点故障。NIST 已确认将向 PQC 业内发布征集提案，以寻求专门填补这一空白。

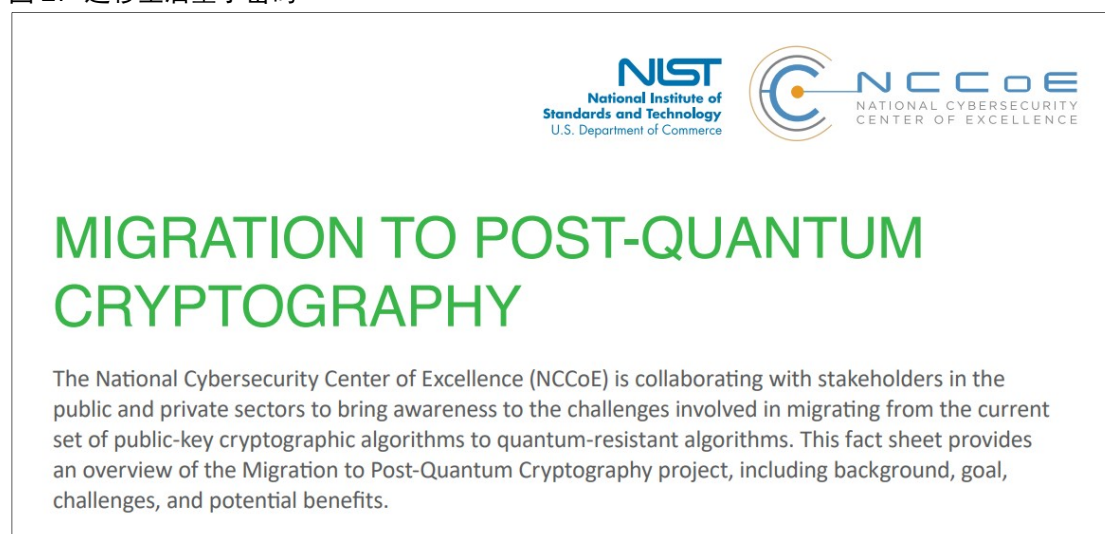
2、迁移是一个更大的挑战

在正式标准完成之前，企业在推广这些新方法时都必须谨慎。然而，为标准文档选择的协议的知识将成为活动的转折点。

互联网是一个疯狂且多样的地方。并非所有协议和硬件都可以在新的更大的密钥和所需的处理开销下顺利运行，尤其是旧硬件和旧应用程序。迁移准备和测试对许多公司来说都是一个具有挑战性的问题。在物联网设备不断增长的环境下，仍然存在一种危险的诱惑，即选择推迟对安全性能采取行动以选择更轻的重量和更高功率的设备。

NIST 国家网络安全卓越中心（NCCoE）现已启动了“迁移到 PQC”项目，以帮助企业规划和执行这种迁移。这是至关重要的一步。如今，大多数黑客攻击的都是实现中的漏洞，而不是底层协议。通过迁移到量子安全协议的仓促或错误想法实际上可能会使这种情况恶化。总的来说，我们对加密安全的理解在过去二十年里不断发展。我们现在更清楚地意识到安全是一个旅程，而不是一个目的地。大多数公司会将加密灵活性置于他们现在想要构建的系统的核心。

图 27 迁移至后量子密码



加密繁荣时期——PQC 迁移活动有望成为网络安全服务提供商的大生意。

IBM、微软和 Atos 等大公司都密切参与了 NIST PQC 进程。许多专业公司都致力于帮助实现 NIST 套件中的算法，包括 PQShield、PQSecure、CryptoNext 和 ISARA 等。

Quantropi 提供自己专有的 PQC 解决方案 QiSpace。这包括 MASQ（多变量 PQC KEM）及其专有的“quantum permutation pad”技术。这受到量子计算架构的启发，但在经典处理器上实现。这被用作其对称加密 QEEP 的基础，并提供伪 QRNG。

Post-Quantum 专注于身份和安全应用程序。EvolutionQ 在提供 PQC 和量子密码学的见解方面具有独特的地位。

那些已经计划开始制定后量子迁移战略的企业可能希望早点开始行动。专家资源是一种稀缺商品，而且将变得更加稀缺。

三、量子密码提供了一个不断发展的工具集

量子技术还为网络安全提供了新工具。这包括帮助应对未来量子计算机构成的威胁，以及更常见的当前威胁。正如我们稍后将看到的，它还承诺提供面向未

来的新功能。

为了理解这些可能性，我们必须研究量子随机性提供的独特属性，了解它是如何实现新的带外加密解决方案以及量子密钥交付的额外独特承诺。我们将看到，在其最强大的用例中，量子密码并不作为传统的基于数学的密码的竞争者，而是对其进行补充和增强。

1、量子随机性很重要

随机数是所有加密系统的基本构建块。它还可用于游戏和数据科学应用。传统系统通常使用基于数学的伪随机数发生器结合一些硬件随机种子值。与来自量子计算机的任何未来威胁完全不同，这些算法或其实现中的漏洞一直是一个反复出现的问题。著名的例子包括台湾“公民智能卡”数据库中的漏洞和 Reductor 恶意软件攻击。目前互联网上使用的 RSA 数字证书中有很大部分被认为容易受到这种方式的攻击。

看好熵（熵可以被认为是随机性的数量，或者等同于信息的缺失）的人认为，升级的随机性是一种有用且具有成本效益的增强。作为更广泛的量子安全迁移策略的一部分，这也是一个需要及时解决的问题。最有安全意识的人还注意到，格加密协议的安全证明非常重视把高质量的随机性作为基本输入。而反对的人认为有其他的优先事项，并质疑如何才能证明支出额外资金的合理性。

量子随机性——随机测量结果是量子力学固有的。事实上，量子系统是我们所知的自然界中唯一表现出真正随机性的事物。

基本的 QRNG（量子随机数发生器）设备是许多量子领域参与者早期盈利的机会。一系列设备已投放市场。通常比其他物理随机性源提供更高的性能，并且承诺它们的输出是真正随机的。

IDQ、国盾量子 and QuintessenceLabs 为市场提供 QRNG 解决方案。初创公司 Quside 正在销售一款基于 FPGA 的产品。KETS 强调了其原型在低 SWaP 环境中的演示。东芝新的集成加密芯片展示了令人印象深刻的 4 Gbps

随机数速率。

IDQ 一直是嵌入式应用小型化 QRNG 的早期领导者。SK 电讯已售出超过 45 万部包含 IDQ 的 Quantis QRNG 芯片的三星 Galaxy A Quantum 智能手机。继此成功之后,还推出了更新的三星 Galaxy Quantum 2。支持 Quantis 的 Vsmart Aris 5G (越南) 正在美国上市。Quantis 也在寻找进入许多嵌入式应用的方法, 这些方法中包括与物理不可克隆 (PUF) 芯片一起用于物联网身份验证。

国盾量子和中国电信也试行了“量子加密”手机解决方案。这可能是基于 sim 分布式量子随机数和基于对称加密的智能手机应用程序。

在第一波 QRNG 实施中, 我们必须相信制造商的芯片正在按照他们所说的那样做。行业采用者希望至少得到认可的保证和认证流程。ITU-T X.1702 是 QRNG 架构的初步建议 (更多人认为基本定义)。

英国国家物理实验室正在领导 AQuRand——一个由英国皇家研究院资助的项目——旨在定义 QRNG 的保证流程。然而, QRNG 市场开始显得拥挤 (仅英国就有七个商业参与者)。在尺寸、重量、功率、随机比特率和成本方面的竞争差异, 也将与更高级功能的差异相结合。

高级协议 (Advanced protocols) ——量子随机性不是一个松散的概念。我们可以进行实时统计测试, 以验证设备是否以独特的量子方式运行 (例如违反贝尔不等式)。这为量子设备证明它们正在产生真正的量子随机性打开了大门。更高级的协议可以让运营商在使用时验证量子随机数 (因此他们不需要信任设备制造商)。在其最完整的形式下, 我们可能能够实现远程和公开地执行协议来形成公开认证的量子随机数。

X.1702 根据验证指定熵的传递方式确定了两类 QRNG 设备: QES1——通过监控实施缺陷是否在容许范围内; QES2——通过测量量子过程的签名。后一种情况是对量子随机性的持续性自我验证, 是一种更为严格的测试。

Quantinuum (前身剑桥量子) 的 SaaS 产品 Quantum Origin 是第一个实施强 QES2 式熵验证的 QRNG 产品。以前名为 Ironbridge, 剑桥量子已经展示了它与

IBM Key Protect 套件作为加密密钥源的集成，最近还与富士通进行了概念验证 PQC VPN 部署，并与 IDB Lab 和 Tec de Monterrey 进行了量子安全区块链部署。Quantum Origin 目前在霍尼韦尔的 H 系列量子计算机上运行，但在任何通用量子计算硬件上都可以运行。

量子计算机似乎是一种非常昂贵的产生随机数的方法。然而，熵验证是黄金标准应用的有效区分因素。此类服务未来可能是专门的低成本专用设备，但这些设备尚未投入生产。这项服务现已推出。

新的参与者 Quantum Dice 计划寻求芯片级解决方案，它强调其 DISQ 协议能够提供高级自我认证。Anametric 也是如此。希望他们重点关注专门针对 PQC 需求量身定制高级协议的方法。我们可以期待听到更多的行业新人的声音，包括 Nu Quantum 和 Quaid。

QRNG 作为领先的量子技术被低估了，但这种情况正在发生转变。量子芯片进入手机等无处不在的消费设备，对整个行业来说都是一笔大买卖。同样，通过私人甚至公共认证为量子随机数增加价值的能力可能是专业量子计算机的首批真正商业应用之一。

2、带外密钥传递

如果我不想信任公钥基础设施，一个自然的替代方法是找到一些其他方法来跨位置传递共享密钥。

TLS handshake——互联网（以及许多企业安全）目前建立都在 TLS handshake 之上。使用公钥基础设施来认证用户并允许他们同意共享密钥。为了方便和灵活，这一切都是在“带内”完成的，在同一通信信道内发送数据。

另一方面，如果我将密钥“带外”传递给将用于数据的通信信道，那么我就大大复杂了对任何攻击者的挑战，尤其是对“现在窃取，以后解密”的攻击。

在高安全性应用程序中，带外密钥传递并不是什么新鲜事（想想在外交公文包中交付的装满随机数的硬盘）。现代技术正在提供新的方法来使这个过程更加

高效。带外解决方案不必使用量子密码学技术。然而，在现在进入市场的新解决方案浪潮中，我们经常看到它们的结合，无论是现在还是未来的升级路径。

Quantum Xchange 是先行者，它的 Phio TX 解决方案是用于按需分发临时的带外密钥（不需要密钥存储）。Phio TX Hive 支持各种交付机制，包括基于云的 VPN。现在可以仅使用传统密码学的技术来实现；同时它还未来多个量子加密选项提供了升级路径。Quantum Xchange 强调，这种逻辑解耦和灵活性对于未来完全的加密灵活性是必要的。他们已经成功完成了与 Verizon 的概念验证，以及将一艘船与美国和澳大利亚的高灵敏度位置连接起来的基于卫星的演示。

在这个基于数学和基于物理的密码学家经常出现争执的领域中，出现了混合系统的创新。这些将基于物理的 QRNG 与基于数学的高级技术相结合，有望在全球范围内大规模分发秘密共享的随机数。

Qrypt 利用 QRNG 信标的网状结构。BLAST 协议允许任意两个客户端秘密同意这些随机数的共享段，以安全地提取共享随机数。这个协议非常简单，可以通过最安全的 PQC 进行协调（例如，rodo KEM）。但它也可以生成大量的密钥材料，使其甚至可以为 OTP 加密提供实际的支持。由于这些随机数是在不同的时间形成的，并且通过不同的信道传输到以后的数据，因此“现在窃取以后解密”的攻击变得更加困难。

Arqit 提出了一个卫星网络，通过任意两个地面站之间的量子下行链路分发共享的量子随机数。对称密码术保护这些数字与密钥的协调。至关重要的是，随机数永远不会通过地面信道，因此传输是完全带外的，并且还受到下行链路的物理量子特性的保护。Arqit 的 QuantumCloud 协调使用这些密钥来保护受完全对称加密保护的网路中的数据中心和用户端点节点。客户现在可以探索该系统的地面实现。第一颗卫星预计将于 2023 年发射。

五眼联盟正在研究 Arqit 系统的一个私有实例——联合量子系统（Federated Quantum System）的潜力，以满足他们的需求。2021 年在英国康沃尔举行的 G7 会议上几个与北约结盟的政府表达了它们的兴趣。其中包括美国、英国、日本、

加拿大、意大利、比利时和奥地利。这是基于 Arqit 在英国研究与创新局 (UKRI) 支持的更广泛的量子密码应用上所做的工作。

安全和创新并非易事。早期采用者应该参考已建立和即将到来的标准（例如 NIST）；信誉良好的期刊/存储库（例如 IACR）中发布协议和安全证明；蓝筹客户的概念验证演示，特别是在国家计划和/或国家实验室的参与允许独立专家参与的情况下的。

3、量子密钥分发（QKD）基本成熟

量子技术还可以用于在两个位置之间提供量子信道。利用量子信号的非经典特性为密钥分发提供新工具。

量子信道——QKD 可以作为带内或带外解决方案。在任何一种情况下，其独特的安全声明都是基于无法克隆量子态的事实。窃听者根本无法在不被检测到的情况下复制和存储量子信号。

P&M QKD——在最简单的“制备和测量”（P&M）形式中，QKD 仅取决于量子不确定性和量子叠加原理。这提供了与传统的基于数学的系统完全不同的安全保证。现实世界的系统可能仍然存在漏洞，但是，不可克隆定理意味着 QKD 只能在传输过程中实时受到攻击，因此可用于提供独特持久的安全承诺。今天几乎所有可用的商业 QKD 系统都实现了这种技术的一些变体。

纠缠 QKD——QKD 的最高级形式直接采用量子纠缠。这使得我们不必非得通过对中间设备制造商和运营商的信任，可以显著提高安全承诺。

安全性证明——相对于许多其他类型的物理层防御，QKD 一个微妙优势是其安全性可以被形式化和数学分析。在其最强大的实现中，QKD 可以提供信息理论上的安全性。

可信节点——由于量子信号传输范围有限，而且目前没有强大的量子中继器来扩大原生量子信号的范围。因此依靠可信节点作为中继，这是安全性中的一个潜在弱点。

过去，QKD 的主要缺点是早期系统相对不成熟和成本非常高。现在这已经不是问题了。如今，覆盖范围、密钥速率以及量子连接在传统基础设施上路由的灵活性已经成为至关重要的考虑因素。

世界各地的 QKD 部署差异显著。

中国拥有迄今为止世界上最大的 QKD 运营网络。2000 公里纵向骨干网连接北京、合肥、济南、上海的城域 QKD 网络；其中济南是最大的，有 50 个终端节点。该网络使用了 700 多条光纤链路和 32 个可信节点中继站。安全密钥速率在 20-30kbs 的范围内。中国的设备越来越成熟，已经可以抵御 28 种已知的潜在物理攻击。合肥和武汉之间 700 公里的额外横向主干道已经完工，还有 360 公里在建，2200 公里拟建。

科大国盾量子技术股份有限公司 (QuantumCTek) 是为中国不断增长的量子网络提供硬件的量子独角兽。其骨干网 QKD 产品包括 QKD-PHA300 (50kbs@损耗 10dB, 最大范围 100km) 和 QKD-POL1250 (80kbs@损耗 10dB, 最大范围 100km)。

SK 电讯 (SKT) 已经将其 LTE/5G 骨干网 QKD 扩展到超过 330 公里，包括使用 5 个可信节点站的首尔-大田-太平核心网络枢纽。SK Broadband 公司和 IDQ 已签订合同，为韩国 48 家政府机构建设一个 2000 公里的 QKD 网络。

IDQ 是量子通信领域的先行者，其总部位于瑞士，自 2007 年以来一直提供商业 QKD 系统。该公司新推出的 Cerberis XG QKD (2kbs@损耗 12dB, 标称范围 50km 可能达到 80km) 强调了部署和操作的方便性。SKT 已经收购了 IDQ。

英国电信 (BT) 和东芝 (Toshiba) 宣布了一项联合项目，在伦敦 (包括伦敦码头区、伦敦金融城和 M4 走廊) 建设和试用商用 QKD 网络。这建立在他们在英国量子网络测试平台以及英国国家复合材料中心 (NCC) 的点对点商业解决方案中合作经验的基础上。东芝还在美国与芝加哥量子交易所建立了 200 公里的量子网络，与日本情报通信研究机构 (NICT) 在日本建立了一个试验台，以及与总部位于新加坡的 SpeQtral 合作，为东南亚的潜在客户提供服务。

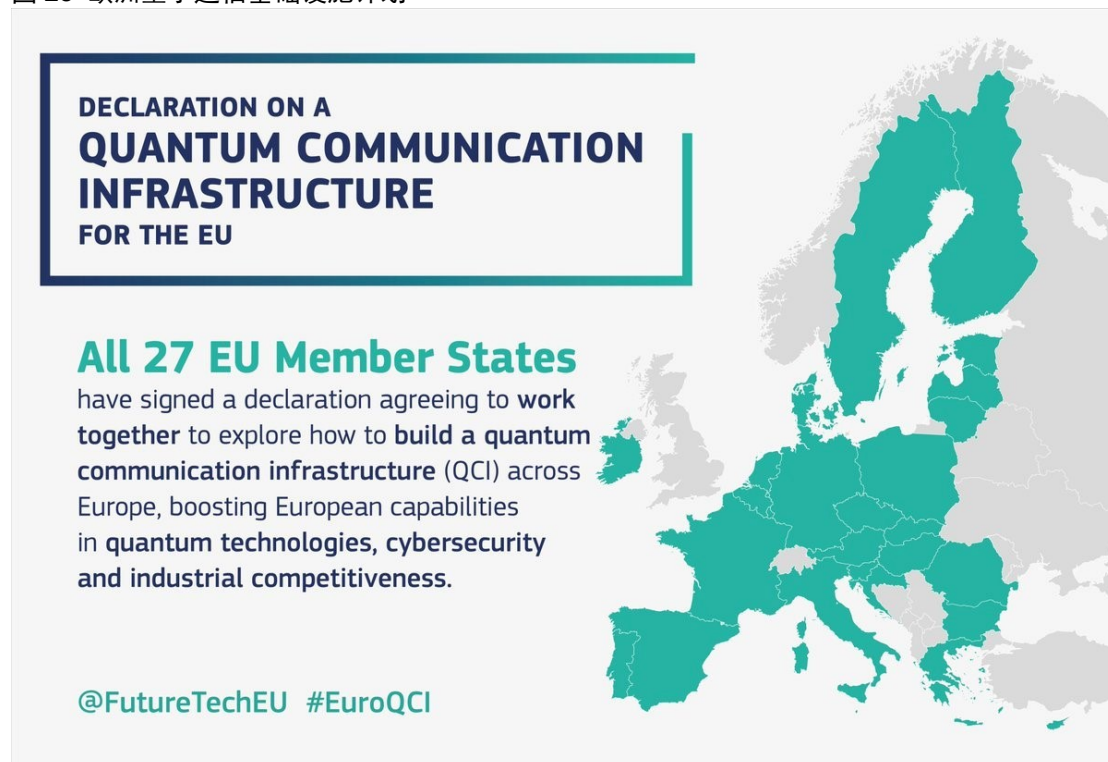
东芝目前在 QKD 范围和性能方面处于领先地位。它们提供了“长距离”解决方案（300kbps@损耗 10dB，标称范围 120km 最大 175km）；以及“多路复用”系统，其优势在于允许在 C 波段（40kbps@损耗 10dB，标称范围 70km）中复用客户数据。

英国电信和东芝在伦敦取得的成功将非常有趣。Quantum Xchange 花了 2 年时间在纽约试用其 Phio QX QKD 解决方案，然后将其战略转移到 Phio TX。伦敦的努力将受益于最新一代东芝 QKD 套件更高的功能和英国电信的客户覆盖范围。这足以改变现状吗？

在国际量子密码会议 QCrypt 2021 上，东芝指出，“国家光纤 OKD 网络今天已经可以实现”。对于英国这样的国家，现有的电信网络核心节点通常位于主要城市。这些位置已经是适用于可信节点实现的严格控制的位置（今天已经被这样使用）。英国的量子产业集团 UKQuantum 已向政府建议创建英国量子通信基础设施。最初提议的骨干网将在五年内连接 6 个主要的大都市中心。

在欧洲，所有 27 个欧盟国家都加入了欧洲量子通信基础设施 EuroQCI 倡议，其具体目标是建立泛欧安全量子通信基础设施。ESA（欧洲航天局）正在协调 EuroQCI 的空间部分（尽管英国和加拿大是 ESA 的成员，但它们被排除在 EuroQCI 参与之外）。OpenQKD 在欧洲建立了 14 个测试平台中心，以展示各种用例。其中包括电信骨干网和云数据中心等核心领域，以及智能电网、电子健康和电子政务等发人深省的应用（英国已通过剑桥测试平台参与了 OpenQKD）。

图 28 欧洲量子通信基础设施计划



VeriQloud 公司正在开发标准 QKD 技术的有趣变体。Qline 是 P&M QKD 的一种形式，它在一次光纤运行中引入了中间节点。每个中间节点可以使用简化的硬件来修改量子信号。任何一对节点都可以形成共享密钥，而无需信任任何其他节点。这只在相对较短的范围内起作用，但有可能提供成本优势，因为许多用户可以通过一次短距离光纤服务。该系统的原型已经准备好部署在柏林 OpenQKD 测试平台上。

在世界其他地方，俄罗斯和澳大利亚在 QKD 开发方面尤为活跃。

俄罗斯初创公司 QRate 提供 QKD312 (50kbps@损耗 12dB，标称范围 30km 最大 120km)。该公司的设备是俄罗斯国立科技大学 (NUST MISIS) 和莫斯科通信和信息学技术大学 (MTUCI) 之间的试验台网络的基础。

澳大利亚网络安全公司 Quintessecelabs 提供 qOptica 100, 使用的是连续变量 QKD (CV-QKD) (上面讨论的其他系统使用的是离散变量 DV-QKD)。CV-QKD 提供了更高的理论效率，但是当前实现的实际速度比 DV-QKD 低得多，目前在

实践中的密钥速率更低、范围更短。Quintessence 并没有公开 qOptica 100 的密钥速率。（作为对比，CV-QKD 的学术现场试验为 6kbps@损耗 12dB）。CV-QKD 的支持者指出，QKD 与标准光学元件的兼容性增强，在日光、自由空间条件下具有优势。我们可以期待这项技术的进一步发展。

上海循态量子科技有限公司（XT Quantech）是一家中国初创公司，也提供 CV-QKD 技术。密钥率为 25kbps@损耗 10dB。

尽管美国是这项技术的早期先驱，但在 P&M QKD 中明显缺席，而是选择强调基于纠缠的技术。

Qubitekk 是一家美国初创公司，利用其纠缠光子源技术提供量子数据链路。它使用纠缠 QKD 来提供独特的安全保证，尽管目前的范围仅限于 1 公里。如今，这似乎是一项很难使用的技术，但这种方法具有长期前景。

东芝目前在 QKD 市场拥有强大的主动权。他们当前一代的套件在任何可用系统的光纤链路上都具有最高的性能。研究也非常强大，其英国研究团队发明的 TF-QKD 协议承诺将实用的 QKD 扩展到长达 500 公里的城际距离。东芝不久前还利用 UKRI AQuaSec 项目实现了一种芯片级解决方案——在光子芯片中结合 QRNG 和 QKD 功能。安全密钥速率令人印象深刻（470kbps@10km）。

KETS 是芯片级 QRNG 和 QKD 解决方案的另一个先行者。其原型现在处于卡片/机架阶段，KETS 是 AQuaSec 项目的另一个合作伙伴。KETS 的创始人仍然保持着他们早期演示芯片的安全密钥速率记录（916kbps@20km，使用片外激光源和 SNSPD）。

中国在 TF-QKD 研究方面处于领先地位，保持着光纤量子密钥分发距离的世界纪录。

2021 年 6 月，中国科学技术大学潘建伟及其同事张强、陈腾云与济南量子技术研究院王向斌、刘洋等合作，利用时频传递技术实现了现场 511 公里 TF-QKD。

2022 年 1 月，郭光灿院士领导的中国科学院量子信息重点实验室的韩正甫教授及其合作者王双、银振强、何德勇、陈巍等基于 TF-QKD 实现了 830 公里

光纤信道量子密钥分发。

2022 年 5 月，潘建伟、张强、王向斌、刘洋等合作，实现了一套融合量子密钥分发和光纤振动传感的实验系统，在完成光纤双场量子密钥分发 (TF-QKD) 的同时，实现了 658 公里远距离光纤传感，定位精度达到 1 公里。

4、标准在成倍增加

与任何技术领域一样，尤其是在密码学领域，我们可以期待标准在赢得商业信心方面发挥关键作用：用于设备制造方式的保证测试，作为认证机构（如国家实验室或测试机构）认证的基础；证明特定级别的保证和认证足以满足业务目的认证；为了便于用户验收，测试系统是否适用于实际操作。

量子密钥分发 (QKD) 的标准化活动正在三个主要机构之间进行，即国际电信联盟电信标准分局 (ITU-T)、欧洲电信标准化协会 (ETSI) 和国际标准化组织/国际电工委员会 (ISO/IEC)。

ITU-T 发布的建议包括：

X 系列（数据网络、安全）：X.1702、X.1710、X.1712、X.1714

Y 系列（互联网、下一代）：Y.3800、Y.3801、Y.3802、Y.3803 和 Y.3804

也叫 FG-QIT4N——网络量子信息技术焦点小组。

ETSI 公布的一系列规范包括：

GS QKD 015、GS QKD 014、GS QKD 012、GS QKD 011、GS QKD 008

GS QKD 016 即将推出，此“保护配置文件”是 ISO/IEC 认证流程的重要环节。

ISO/IEC 正在进行多项活动：

JTC 1/SC 27 (IT 安全技术) 致力于 CD 23837 第 1 和 2 部分

还有 JTC 1/WG 14 (量子计算) 致力于 AWI 4879

5、数学与物理之间的紧张局势持续发酵

数学家和物理学家多年来一直在争论 PQC KEM 和 QKD 各自的优点。NSA 和英国 NCSC (GCHQ 的一部分) 都警告不要过早采用 QKD 技术。然而私下里, 许多物理学家对以数学为主导的加密机构叫屈不已。但一些团体也犯了夸大宣传和忽视 PQC 优势的错误。

对于传统的互联网和“正常的”商业应用, PQC 显然是我们现在可以采用的首选方案。但 PQC 和 QKD 显然也是互补的, 两者都允许我们形成新的灵活的带内协议, 并在需要更高级别的持久安全性时作为分层防御。

确保商业案例支持 QKD 的额外成本是一个重要的考虑因素。在这里, QKD 还必须面对来自传统带外解决方案的成本竞争。

NCSC 最近强调以基于原则的方法来保证安全技术, 这可能是超越过去争论的一种建设性方式。这场辩论也扩大到包括其他地方。英国电信行业监管机构 Ofcom 已经迈出了进入这一领域的第一步。

在中国, 2021 年, 中国科大、国盾量子、国科量子、济南量子技术研究院与上海交大等单位的研究人员完成了全球首次量子密钥分发 (QKD) 和后量子密码 (PQC) 融合可用性的现网验证。

四、太空带来了新的潜力

空间技术正在经历一场革命。大型卫星正在让位给成本效益更高的纳米卫星星座。新的发射方案即将推出。LEO、MEO 和 GEO (低中高轨道卫星) 部署都存在机会, 每种部署都会在区域覆盖与全球覆盖之间进行不同的权衡, 最终可以分担哪些用户群成本。从长远来看, 地月拉格朗日点和月球本身存在独特的机会。

卫星链路可用于扩大近期量子密码学应用的范围。然而, 它们也提供了一种潜在的方法来加速依赖于量子纠缠分发的更高级协议的交付。

1、卫星 QKD 火起来了

从卫星节点发送量子信号本身就非常有吸引力。大气层的厚度只有大约 10 公里，量子信号能够在太空真空中以低得多的损耗传播。该行业还受益于对经典光通信的大量投资。

地月——40 万公里的估计损耗为 80 dB(10 厘米发射器和 1 米接收器@1550 纳米)。这与仅 270 公里光纤的损耗相同 (0.3 dB 损耗/公里)

P&M QKD 的指示性参数

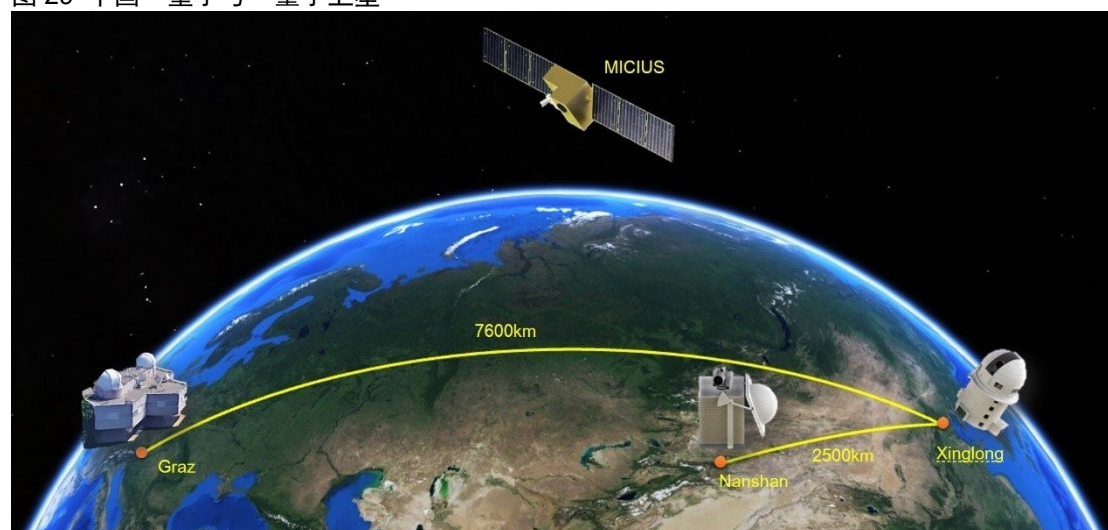
LEO-地面: 130 kbps (1.2GHz, 发射 13 厘米, 接收 80 厘米, <30 度仰角) ;

GEO-地面: 1 kpbs (1.2GHz, 发射 60 厘米, 接收 120 米, 30 度仰角) 。

想要研究卫星 QKD 还有其他重要的原因。安全意识强的用户通常最关心到远程全球位置的链接: 他们无法通过中间可信节点到达的位置。另一方面, 他们可能对他们的卫星充当可信节点感到满意。

中国凭借墨子号卫星开创了量子空间技术的先河。然而, 这是一颗 640 公斤的大型研究卫星, 功率为 560 瓦; 所需的地面站为 10 吨 (目前已有小型化移动地面站), 使用 60 千瓦, 维护成本很高。世界各地的倡议都在竞相为卫星 QKD 开发更具可扩展性和成本效益的平台。

图 29 中国“墨子号”量子卫星



微型量子卫星——中国计划到 2021 年底在低地球轨道上拥有一颗 100 公斤的微型卫星，到 2022 年将增加到 2 颗卫星和 10 个地面站。目标是快速架设 100 公斤 300 瓦地面站。已经在北京、上海和重庆进行了实地试验。

ROKS——英国的一项任务，旨在在 2022 年展示 QKD 下行链路。合作伙伴包括 Craft Prospect 和 Fraunhofer。

QEYSSat——这项由加拿大主导的任务将于 2022 年发射，主要目的是展示卫星的量子上行链路。作为英国-加拿大量子技术计划协议的一部分，包括 Craft Prospect 在内的英国财团正在提供额外的下行链路源。

Speqtire（以前称为 QKD Qubesat）——英国和新加坡之间的联合 QKD 测试平台任务由卫星制造商 ISISPACE 建造。发射日期现在已经推迟到 2023 年以后。它建立在 2020 年的任务 SpooQy-1 的基础上，该任务成功完成了 CQT（新加坡量子技术中心）纠缠光子源的在轨测试。

英国量子通信中心（UK Quantum Communications Hub）正在寻求从立方星到英国地面站的 QKD 的单独在轨演示（IOD），计划于 2024 年发射。

QKDSat——Arqit 和 ESA（欧空局）的一个项目计划在 2023 年使用维珍轨道公司的发射器发射两颗卫星，其中一颗来自康沃尔郡的 Newquay，以支持其 QuantumCloud 服务。这些卫星将在 Harwell 的英国国家卫星测试设施进行集成和测试。随后可能会有更多的 FQS 卫星。

SAGA——一项 ESA（欧空局）计划的任务，旨在展示基于纠缠的 QKD，并有望在现有欧洲进展的基础上再接再厉。德国 QUBE 和法国 Nanobob 均预计 2022 年发射。Qtlabs 正在协调任务设计和技术选择。这是 EuroQCI 的主要空间部分，预计将与欧洲量子旗舰计划进行紧密合作。

传统的带外卫星解决方案，例如 Quantum Xchange 的 2021 年概念验证也将得到扩展。

星座设计的一个重要机会是允许全球用户分摊成本。现在，一个光学地面站的成本可能约为 100 万欧元，但如果批量生产，成本可能只有 10 万欧元。一颗

专用的量子卫星可能耗资 1 亿欧元，但租用商业卫星服务（可能类似于 Arqit 的 FQS 提案）可能每年就耗资 2500 万欧元。包括卫星、任务控制和 100 个接收器。此类成本并非微不足道，但对于政府或具有安全意识的大公司而言，也并非无法承受。

关于光纤与卫星 QKD 的距离/成本权衡的争论已经开始。卫星套件似乎很贵，但可以跨越很远的距离并且成本可以分摊。光纤安装看起来更便宜，但成本随着距离的增加而增加。卫星支持者 Qtlab 认为，这种权衡将出现在 200 公里，IDQ 出现在 1500 公里，东芝在 10,000 公里。

2、纠缠分发的敲门砖？

卫星可能是我们可以部署基于纠缠的 QKD 的首批领域之一；只要两个地面站同时可见，就不需要信任卫星。在 ICQT 2021 上，中国科大的徐飞虎推测实用的地面量子中继器可能还需要 10 年的时间。另一种选择是使用卫星，中国科大已经演示了使用卫星在 1120 公里范围内的纠缠分发。

纠缠 QKD 的指示性参数（来自 Qtlab）

LEO 对地：25bps（1GHz 对速率，发射 13 厘米，接收 80 厘米，<30 度仰角）

GEO 对地：0.1bps（1GHz 对速率，发射 60 厘米，接收 120 米，30 度仰角）

重要的是，卫星系统可以加速实际的基于纠缠的链路的部署。这样，它们将有许多其他用途。

五、未来的量子网络即将出现

1、量子网络指数级地增加量子计算机的能力

对网络安全的讨论自然地将我们从后量子密码引导到量子随机数，再到用于创建量子安全密钥的协议。但量子网络的潜力并不止于此。长期来看这些甚至不是主要的好处。

在短期内，短距离量子网络的一个关键驱动因素将是相干连接本地量子处理器（例如在稀释制冷机或俘获离子架之间）。然而，这种组合的本质优势并不受距离的限制。

经典计算机联网，它们的能力呈线性增长。当我们纠缠量子计算机时，它们的能力呈指数级增长。独立和统一量子处理器之间的能力差距可能会为建立真正基于纠缠的量子互联网提供强有力的案例支持。

2、高级密码协议的持续进展

量子通信领域还提供了一系列高级加密协议，有望扩展基于传统数学技术的可能性。

Stephen Wiesner（1942-2021 年）——为现代量子信息领域尤其是量子密码铺平道路。他写于 20 世纪 60 年代末但直到 1983 年才发表的关于共轭码的论文为我们现在所知的量子比特铺平了道路。

近年来，在更实用的协议和实验演示方面都取得了稳步进展：

表 2 高级密码协议

不经意传输（存储器带有噪声） ——一个重要的原语	实验演示
比特承诺（具有信令约束） ——一个重要的原语	24 小时相对论比特承诺
量子数据锁定 ——以指数级更短的密钥长度取代 OTP 加密的潜力	实验演示
量子数字签名 ——用于身份验证和不可否认性的量子协议	超过 102 公里的实验演示
量子货币 ——不可伪造，可验证的代币（数字货币，区块链等）	半设备独立协议；S-money 使用信令约束来避免对量子存储器的需求。初步实验结果于 2021 年得到证实。

通用盲量子计算 ——云安全的量子计算	“简洁”盲量子计算协议
一次性程序（具有概率假设） ——软件许可，一次性授权，电子投票	一次性程序的原理验证演示
掷硬币 ——领导人选举，共识协议	安全弱掷硬币协议（每一方都有一个首选结果）
量子位置验证 ——地理位置证明	新的容错协议（未纠缠攻击）
安全时钟同步 ——精确、无干扰的远程时钟同步	超过 7 公里光纤的实验演示
零知识证明 ——身份验证	使用光子处理器演示 NP 证明验证

NP 证明验证——2021 年，来自 CNRS、爱丁堡大学和 QC Ware 的一个团队实现了 NP 证明验证的真实世界演示，其中证明者仅获得有关他们被要求验证的解决方案的有限知识。这使用简单的双模式光学装置（相当于 1 量子比特计算机）。这是经典密码学中一个经过充分研究的工具——零知识证明的量子变体。这没有直接的应用，但很可能在未来的量子互联网中用作识别、身份验证和区块链等功能的原语。更有趣的是，它提醒我们，通信协议中的“量子优势”甚至可以基于一个 1 量子比特的设备。

Quantum Blockchains 是一家波兰初创公司。它们为将 PQC 技术与量子增强协议相结合可能实现的创新提供了一个有趣的、面向未来的例子。

即使在今天，出于数据隐私的考虑，一些客户已经开始寻求在内部安装量子计算机。盲量子计算提供了在云计算环境中完全有效地解决隐私问题的工具。

3、联网量子传感器的突破？

另一种可能性是将量子传感器连接到量子网络。在 2021 年，量子物互联网得到了显著的提升。包括加州理工学院和谷歌在内的工作表明，如果我们在应用经典机器学习之前，首先在量子计算机中完成预处理，那么在学习量子态的性质

方面会有指数优势。

从实验中学——加州理工学院和谷歌的工作要求我们分两部分考虑谷歌的 Sycamore 量子处理器。

首先第一部分，它的量子比特代表一些假设物理实验的输出（或一系列量子传感器的输出）。我们的任务是了解这种状态的一些特性（研究实验的物理特性，或者读取我们的传感器网络）。量子处理器的其余部分在将输出传递给经典机器学习例程之前，对这些输入执行纠缠操作。这种设置能够在比任何经典算法都少的指数级试验中学习状态的性质。

一个显著的特点是指数优势不依赖于以任何方式预先纠缠的输入状态。这可能与我们的预期相反，并且使得实现这样的设置看起来比我们预期的要容易得多。

这些新结果可能会为基础物理实验中的新分析方法带来短期机会。从中长期来看，它为联网量子传感器可能实现的目标开辟了有趣的可能性。

4、实验室中的纠缠网络

量子纠缠通常首先在量子计算的一般介绍中讨论，或者作为高级形式的 QKD 的促成因素。然而，它的作用远不止这些应用。纠缠是未来量子互联网的重要的可消耗资源。

量子态隐形传态——如果我们在位置 A 和 B 之间共享纠缠，那么我们可以使用它来将任意量子比特从 A 传输到 B，只需发送一个简单的经典信号。无论距离如何，这都有效。

量子中继器——这项新兴技术旨在扩大我们可以共享量子纠缠的范围。典型的中继器设计需要量子存储器（是一个刚刚从实验室兴起的领域）。最近，基于光子图态提出了替代的无存储器方法。

世界各地正在发生越来越令人印象深刻的纠缠网络演示。这些越来越多地突破纯物理领域，以解决工程的实际问题。

中国科大已经在 22 公里的距离上证明了量子存储器的纠缠。他们还展示了

使用光子团簇态作为基于物质的量子存储器的替代方案。

2020 年，英国量子通信中心的合作伙伴布里斯托大学演示了 8 节点网络上的纠缠分发。量子旗舰项目 UNIQORN 展示了灵活交换纠缠共享所需的 q-ROADM 技术。2021 年，赫瑞-瓦特大学的一个团队演示了四个节点之间基于纠缠的量子会议密钥协议。QuTech 则更进一步，演示了通过一个中间节点进行纠缠交换，形成一个 3 节点量子网络。

QuTech 使用了三个金刚石 NV 节点（每个节点冷却到 4K），每个节点包含一个用于通信的量子比特。中间节点使用了一个额外的存储量子比特。虽然只是实验室规模的演示（节点相隔 30 米和 2 米），但这种设置复制了量子中继器的关键功能。这提醒我们，量子通信中的应用将利用并不总是需要极端 mK 冷却的硬件平台。

阿贡国家实验室和芝加哥大学已经成功地在 80 公里的网络上纠缠光子。

布鲁克海文国家实验室和纽约大学石溪分校石溪大学正在开发一个专注于开发量子中继器的网络实验台。干涉效应已被证实超过 160 公里。有计划将网络扩展到纽约市。

Qunnect 是一个著名的早期衍生公司，它拥有基于原子蒸汽电池的量子存储专利技术。这保证了室温部署和光纤兼容性。据报道，存储时间已经在数百微秒的范围内。这可能为真正的量子中继器和其他量子互联网协议打开大门。

QuTech 不仅完成了 3 节点网络演示，还部署了一个完整的软件堆栈。各类参与者现在都在推出量子网络模拟产品。

Quantum Network Explorer（量子网络浏览器，QNE）——QuTech 已经推出 QNE 和相关 SDK，其他感兴趣的各方可以出于教育、研究和开发目的访问他们的网络。

Aliro Quantum——一家美国初创公司，他们提供了 Q.Network 来解决网络堆栈问题。他们的硬件无关量子网络设计和模拟平台使他们能够解决 EaaS 如何帮助客户解决安全、计算以及定位、导航和计时问题的前瞻性问题。

NodeQ——一家英国初创公司，提供用于量子网络设计和优化的软件。利用其创始人在英国量子通信中心的工作以及该领域深厚的理论积累。

EvolutionQ——加拿大初创公司，为量子网络设计提供 BasejumpQDN。最初的重点是帮助客户避免与单一 QKD 供应商的供应商锁定。EvolutionQ 在基于数学的密码学方面的优势与此产品相得益彰。

许多人都知道 IBM 在量子计算领域抓住了势头，这是因为它早期提供了 IBM Quantum Experience，并推广了 OpenQASM 等早期标准。然而，它在量子互联网堆栈是否存在类似的机会？

六、策略之争

在构建量子互联网的过程中，投资者、公司和政府面临着复杂的局势，其中三大深层次的技术部门相互重叠和互动：加密、量子 and 空间。避免被锁定在任何一种技术或狭窄的专业领域是一个挑战。评估短期、中期和长期收入机会的权衡是一项挑战；因此，当我们考虑经济与地缘政治因素的相互作用时，可能会影响更广泛的部门的发展。

一些专注于如何在当前互联网上部署量子安全加密技术。另一些专注于使用可信节点构建“制备和测量”量子网络，以形成量子互联网。其他人则设想真正的基于纠缠的量子互联网。这最终还包括量子传感器，从而实现量子物联网。

中国将其目前在早期 QKD 网络中的主导地位视为未来完全纠缠网络的铺垫。EuroQCI 和 QIA 在欧盟数字欧洲计划中的作用似乎体现了相同的愿景。而美国似乎更倾向于直接关注纠缠的目标。

七、展望 2022

- NIST PQC 决策——哪些 PQC 协议将进行标准化？
- NIST PQC 第 4 轮——哪些替代方案将进行进一步研究？哪些新的数字

签名方案将进入流程？

- QRNG 智能手机——这一细分市场会继续增长吗？
- QRNG 功能之争——在日益拥挤的细分市场中，在成本、随机比特率、

SWaP 和高级协议功能方面的竞争。

- Quantum Xchange——建立了带外概念后，我们将看到哪些客户采用？
- Qrypt——我们会看到这种有趣的新方法的旗舰装置吗？
- Arqit——我们会看到更多细节和安全证明进入公共领域吗？
- 东芝和英国电信——我们会听到伦敦 QKD 试点客户的消息吗？
- IDQ——韩国之后的下一站是哪里？
- 芯片级 QKD——观察来自东芝和 KETS 的芯片将竞争推向新的前沿。
- OpenQKD——注意欧洲试验台位置的各种用例的概念演示证明。
- EuroQCI——数字欧洲计划下的项目资助，是否会为我们提供有关该计

划将如何进行的更多指示？

- UKQCI——英国是否会承诺推出国家量子通信基础设施？
- 卫星 QKD——随着多颗卫星的发射；谁将赢得演示纳米卫星 QKD 的竞

赛？

● 国际标准——关注美国关于中国在国际标准制定中日益重要的作用的研究结论。

- 保证流程——将 QRNG 保证视为 NPL 和 NCSC 新思维的测试案例。

● 纠缠网络——关注领先的研究中心的进展，如中国科学技术大学、英国量子通信中心、荷兰 QuTech、美国 Q-NEXT/阿贡国家实验室、布鲁克海文国家实验室、MARQI/马里兰大学、CQT/普渡大学等。

● 高级协议——注意对高级协议的新兴趣。云上的安全时钟同步和盲量子计算可能值得关注。

● 欧洲量子旗舰——有影响力的量子互联网联盟将在下一轮地平线欧洲项目拨款中获得哪些支持？

- 网络堆栈——哪个平台将在量子网络模拟方面取得领先？

声明

本报告采用的数据均来自公开渠道或对公开数据进行的整理。本报告发布的观点力求独立、客观和公正，结论不受第三方授意或影响，不构成任何广告。

光子盒全部原创作品版权归光子盒所有。其他媒体、网站或个人转载使用时不得进行商业性的原版原式的转载，也不得歪曲和篡改本网站所发布的内容。如转载须注明来源为“光子盒”，不得对本报告进行任何有悖原意的引用、删减和篡改。未经书面许可，任何机构和个人不得以任何形式翻版、复制或发表。如征得光子盒的同意进行引用、刊发的，需在允许范围内。违规使用本报告者，法律必究。

光子盒引用其他资料的目的在于呈现信息，并不代表光子盒赞同其全部观点，不对其真实性、时效性负责。

本报告具有一定的时效性，仅表达截至发稿时的情况，不代表未来情况。在任何情况下，本报告中的信息或所表述的意见均不构成投资建议。

关于我们



光子盒 (GUANGZIHE) 这一创业理念萌生于 2019 年 9 月，第一篇媒体文章发表于 2020 年 2 月。“光子盒”这一名称来自于在 1930 年第六届索尔维会议 (Solvay Conference) 上，爱因斯坦 (Albert Einstein) 在其与玻尔 (Niels Bohr) 的争论 (Bohr-Einstein debate) 中提出的一项光子盒实验 (photon box experiment)。

光子盒以量子信息技术为切入点，通过文字、视频等方式传播资讯、科普知识、解读技术等。光子盒通过提供商务推广、研究报告、展览会议、投融资、战略咨询等服务，已与中国多地政府、国内外多家研究机构和科技企业建立了良好的合作关系。

成立至今，光子盒积极参与中国量子信息科技领域的重大活动，例如：2021 年 5 月，光子盒作为协办方，与主办方中国电子科技集团公司电子科学研究院、社会安全风险感知与防控大数据应用国家工程实验室和中国工程科技发展战略安徽研究院，在安徽合肥成功举办了“2021 中国量子科技产业‘双循环’高峰论坛”。2022 年 3 月，光子盒为重庆市沙坪坝区政府提供支持，筹建重庆市量子实验室，未来也将持续为重庆量子信息科技行业提供服务和保障。

光子盒正在不断扩充自有量子信息科技产业数据库的广度与深度，建立多维量子产业数据信息，提供客观、专业、深入及具有时效性的前沿科技报道和研究报告等。光子盒未来仍将在前沿科技领域持续发力，为建设中国量子信息科技生态圈做出努力，同中国量子信息科技产业共同



CONTACT US



gzh.marketing@quantumchina.com



www.quantumchina.com



更多精彩内容 请关注光子盒公众号

