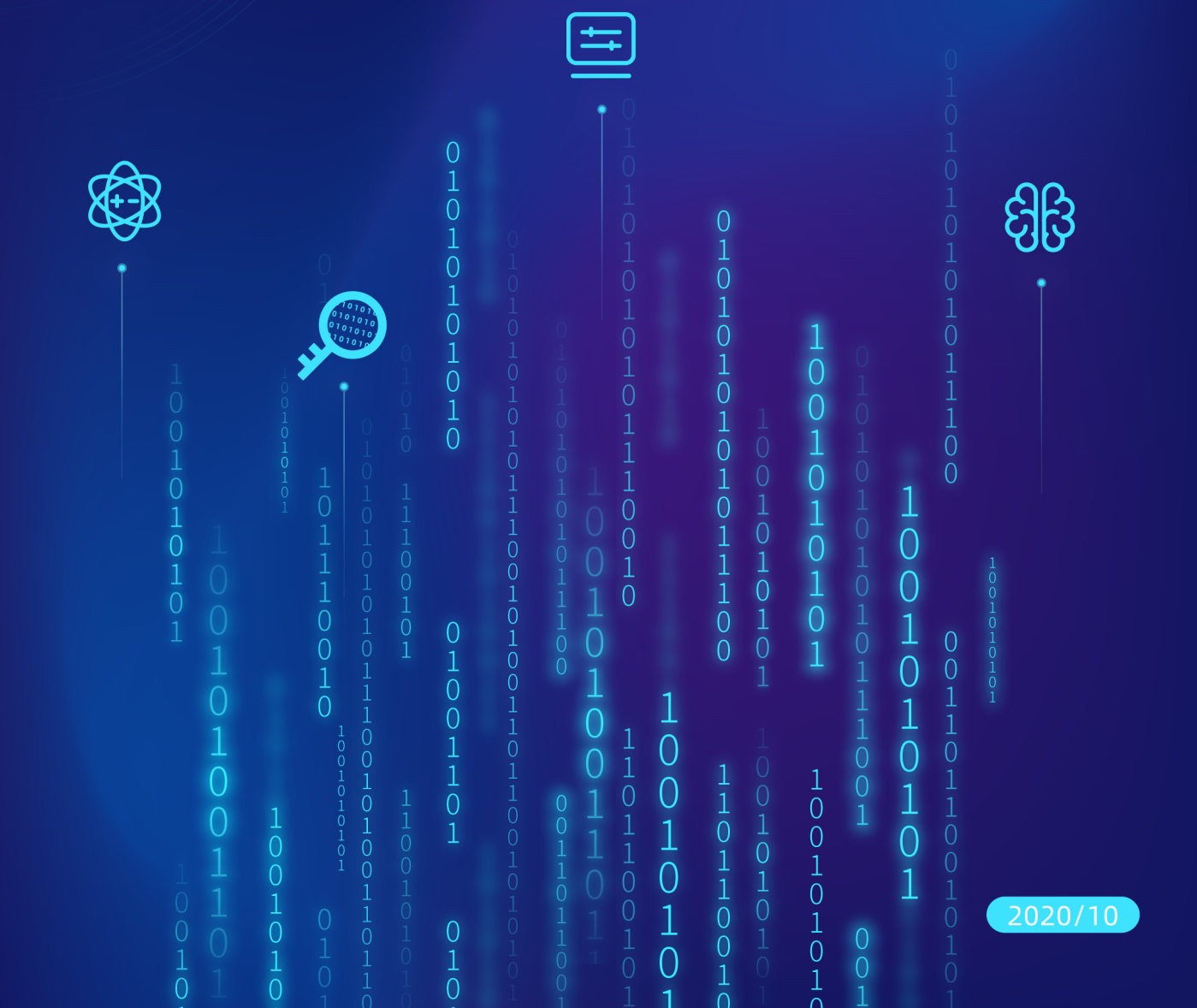
WeBank 微众银行 | 金融科技 微洞察 FISCO金链盟

先手之棋

2020金融量子计算发展报告



2020/10

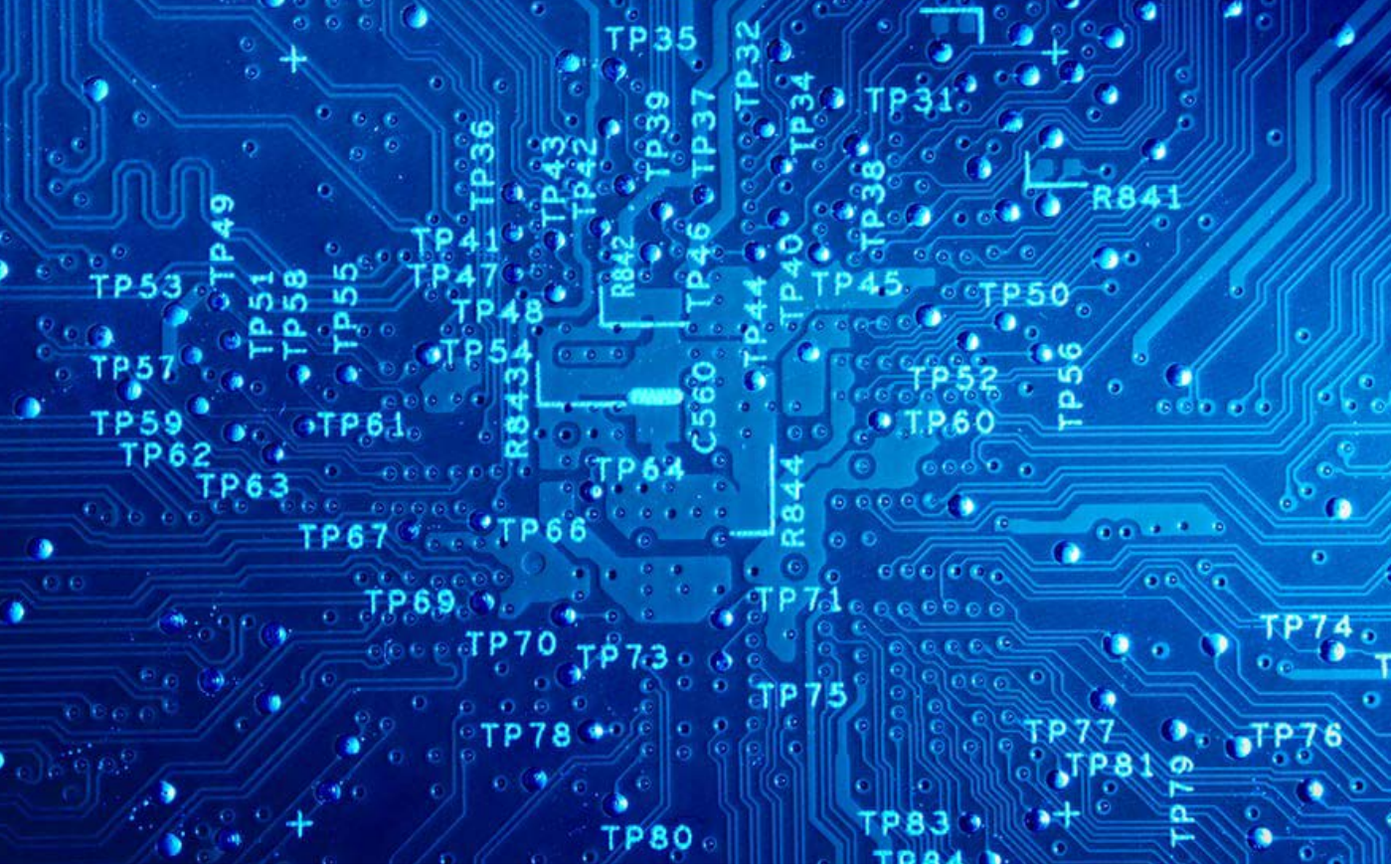
序言 PREFACE

2020年10月16日下午，中共中央政治局就量子科技的研究和应用前景举行第二十四次集体学习。中共中央总书记习近平在主持学习时强调，当今世界正经历百年未有之大变局，要充分认识推动量子科技发展的重要性和紧迫性，加强量子科技发展战略谋划和系统布局，把握大趋势，下好先手棋。习总书记指出，要系统总结我国量子科技发展的成功经验，借鉴国外的有益做法，深入分析研判量子科技发展大势，找准我国量子科技发展的切入点和突破口，统筹基础研究、前沿技术、工程技术研发，培育量子通信等战略性新兴产业，抢占量子科技国际竞争制高点，构筑发展新优势。

本次量子科技的集体学习，是继2017年12月8日的大数据集体学习、2018年10月31日的人工智能集体学习和2019年10月24日的区块链集体学习后的又一个前沿科技学习领域，这或也意味着量子科技将与大数据、人工智能和区块链并肩齐驱，成为数字经济的关键核心技术与核心驱动引擎。

目前，量子科技虽然仍处于发展的初期阶段，但已经引发了各国政府和产业界的强烈关注，国内外科技巨头也已纷纷布局以抢占先机。其中，量子计算作为量子科技的重要细分领域之一，占据着举足轻重的地位。以下，本报告将从金融从业者的角度出发，探讨将量子计算与金融业务深度融合的价值、收益与风险。

目录 CONTENTS



量子计算的发展现状与市场格局

国内外科技巨头争相布局

国内科技巨头已开始争相布局量子计算技术领域，邀请了数名顶尖学者、科学家担任负责人，并仍在全球大力招揽技术人才。华为从2012年开始就专门成立量子实验室，探索量子科技。2018年，华为发布量子计算模拟器HiQ云服务平台。2015年，阿里云与中国科学院共同成立“中国科学院-阿里巴巴量子计算实验室”，开展量子计算的前瞻性研究，联合开发出“量子计算云平台”，这是阿里跨入量子计算领域的第一步。2018年2月，中科院宣布联合阿里云打造11量子比特超导量子计算的云平台。当年5月，阿里达摩院宣布已经开始研发超导量子芯片和量子计算系统。腾讯于2017年12月宣布成立量子实验室，网罗量子相关的算法、复杂性、通讯、模拟、量子物理、量子化学等各方面的人才，有计划跟人工智能技术相结合。百度直到2018年3月8

日才宣布成立量子计算研究所，开展量子计算软件和信息技术应用业务研究。百度计划在五年内组建世界一流的量子计算研究所，并逐步将量子计算融入到业务中。2020年5月，百度飞桨发布量子机器学习开发工具“量桨”(Paddle Quantum)。

国际上，早从2015年开始这场竞赛就已经很激烈了，科技巨头都在量子计算领域投入数千万美元研发，发力量子计算押注十年后的未来。主要的玩家有Google，IBM，Intel，Microsoft等。其中，Intel在2018年年初交付了49量子比特的超导测试芯片，这款芯片代表着该公司在开发从架构到算法再到控制电路的完整量子计算系统方面的“一个重要里程碑”，将使得研究人员能够评估和改进纠错技术，并模拟一些计算问题。2017年年底，IBM成功建成并测试全球首台50个量子比特的量子计算原型机。2020年9月，IBM还发布了扩展量子技术路线图，计划3年内将量子比特数量拓展到惊人的1000个以上。2018年3月，谷歌宣布推出一款72个量子比特的通用量子计算机Bristlecone，在量子比特数目上达到全球第一。2020年初，Google推出了量子机器学习库TensorFlow Quantum，进一步强化量子计算领域的领先地位。Amazon则于2019年底宣布提供量子计算云服务，正式入局量子领域，今年8月将其Braket量子计算云平台推出上市。

全球各国政府高度重视

2018年11月，美国商务部工业安全署（BIS）出台了最新技术出口管制先期通知，根据这份框架，美国政府考虑对14个类别的科技关键领域进行管制，包括人工智能、芯片、量子计算、机器人等被认为涉及国家安全和高技术的前沿科技。此举措可见美国对量子计算技术极其高度重视。

因为具有极为重大的应用价值，量子技术受到了各国政府的高度重视，各国攻关量子计算机的战略已经明确，近年来，多个国家投入巨资启动量子计算研发。美国是最早将量子信息技术列为国防与安全研发计划的国家。作为量子理论的发源地，欧洲高度重视量子信息技术对国家安全、经济发展等方面的影响，投入众多资源大力发展相关技术。此外，日本、韩国、新加坡、加拿大等科技强国均发布了自己的“量子信息科学发展计划”。日本计划10年内在量子计算领域投资3.6亿美元，加拿大已投入2.1亿美元资助滑铁卢大学的量子研究等。

表 1：美国、欧盟、英国在量子计算发展的重大规划

国家	时间	重大事件
美国	2002 年	美国防部高级研究计划局（DARPA）制定了《量子信息科学与技术规划》
		发布 2.0 版，给出了量子计算发展的主要步骤和时间表
	2008 年	DARPA 斥巨资启动名为 “微型曼哈顿计划” 的半导体量子芯片研究计划，甚至将量子计算研究列为与原子弹研制同等重要的高度。
	2016 年	美国国家科学技术委员会发布《推进量子信息科学：国家的挑战与机遇》报告，认为量子计算能有效推动化学、材料科学和粒子物理的发展
	2018 年	《国家量子倡议法案》通过，计划在 10 年内 12.75 亿美元，全力推动量子科学发展；白宫国家科技委员会（NSTC）成立量子信息科学子委员会
	2020 年	公布 “量子互联网计划”；NSF 宣布成立三家量子研究机构，加速量子科技研发
欧盟	2005 年	提出专门用于发展量子信息技术的《欧洲量子科学技术》计划和《欧洲量子信息处理与通信》计划，成为继欧洲核子中心、航天技术后的又一次大规模国际合作
	2018 年	投入 10 亿欧元实施 “量子旗舰” 计划
	2020 年	德国投资 20 亿欧元发展量子技术，欧盟推出第一个公共的量子计算平台
英国	2015 年	英国政府发布了《量子技术国家战略》和《英国量子技术路线图》，将量子技术发展提升至影响未来国家创新力和国际竞争力的重要战略地位。
	2016 年	国政府科学办公室发布量子技术报告《量子技术：时代机会》，提出建立一个政府、产业、学界之间的量子技术共同体
	2019 年	政府宣布投资 1.5 亿英镑于量子计算，并拉动全球公司投资 10 亿镑

我国政府近年在政策上也给予了大力支持与明确指导（见表2）。2017年，我国宣布斥资100亿美元在合肥市建设一个国家级量子科学实验室，将在2020年正式投入使用，该实验室有两个主要的研究目标——量子计量和建立量子计算机。2018年5月，中国科学院也宣布最新成果，由中科大、中国科学院-阿里巴巴量子核算实验室、浙江大学、中科院物理所等单位或公司联合研制的光量子计算机正式诞生。

表 2：我国近年来的量子技术主要政策文件

发布时间	发布机构	政策文件	相关内容
2016 年 2 月	科技部	国家重点研发计划	“量子调控与量子信息” 重点专项
2016 年 3 月	国务院	“十三五” 国家信息化规划	加强前瞻布局，着力构建量子通信，构建量子通信网络发展等重大工程建设
2016 年 7 月	国务院	“十三五” 国家科技创新规划	将量子通信与量子计算机纳入科技创新 2030 重大项目
2017 年 1 月	中共中央、国务院	国家创新驱动发展战略纲要	前瞻布局新兴产业前沿技术研发，如量子信息技术
2017 年 6 月	科技部、教育部、中国科学院、自然科学基金委	“十三五” 国家基础研究专项规划	将量子通信与量子计算机纳入十三五期间基础研究领域拟组织实施的重大科技项目
2017 年 11 月	发改委	2018 年新一代信息基础设施建设工程	提出国家广域量子保密通信骨干网络建设一期工程
2019 年 9 月	济南市	关于加快建设量子信息大科学中心的若干政策措施	城市层面出台的首个量子信息产业政策
2020 年 10 月	政治局	集体学习量子科技	对量子科技的布局和发展提出总体要求

量子计算的技术原理

量子的特性

物理学中描述解释原子、电子、光子等以下层级微观粒子运动规律时，有一套区别于宏观经典物理的世界观和研究体系，被称为“量子力学”（Quantum Mechanics）。日常我们所见的物体都是海量微观粒子在宏观层级的汇聚，可以用经典力学解释，但要深入到微观尺度上，粒子的运动规律与我们的直观认识大相径庭，就需要运用量子的视角来解释和操纵。这些运动规律和粒子的状态不能用经典力学以确定性的方式刻画，因为它是概率性的、内生不确定性的，这些微观粒子组成了一个量子系统。这个量子系统具有以下几条非常独特的性质。

1 **波粒二象性（wave-particle duality）：**一个量子对象同时具有波和粒子的性质，系统的演化状态可以用波的方程表达，但对系统的测度却要用粒子的方式来对待。

2 **量子叠加（superposition）：**一个量子处于不同状态的非常模糊、概率性的叠加态上，可以同时处于多个状态上，测不准其状态。

3 **量子测量（measurement）。**粒子一旦被测量，其状态就会被根本改变，所以量子世界的测量极其困难。

4 **量子相干（coherence）：**如果一个量子系统的各个状态能够被一组复数刻画，那么这个系统处于“相干态”，它是量子满足各种微观性质的必要条件，也有利于人们观察量子。但是如果量子系统被外部环境干扰了，每种状态就会变得概率化，不再保持理想的量子纯态，发生逐渐“退相干”（decohere）。相干性和上一条量子测量的特性表明，要观察和测度量子而不让它被环境破坏，本身就是非常矛盾的。

5 **量子纠缠（entanglement）。**量子世界中不同粒子之间有无法用经典规律理解的整体关联性，不能分开来描述个别粒子，一旦改变某个粒子，会影响到其他粒子。

这5条量子的特殊性质使得量子技术具有传统技术无法匹敌的巨大优点，在计算、加密、仿真等方面都有不同寻常的能力，产生了量子计算、量子通信、量子仿真、量子传感等全新的技术体系。

量子计算的概念和优势

量子计算是量子技术最主要的应用之一。经典的计算机是通过一串二进制代码 0 和 1 来编码和操纵信息，1个经典比特（bit）只能存储0或者1一个值。但量子计算机不同，量子计算机是用“原子”和光子做的。量子计算机运行的物理过程，就是单量子尺度上的原子－光子相互作用。它具有像比特一样携带信息的结构组件，称为“量子比特”（qubit）。量子比特既具有经典计算机的0-1数字电路特性，又因为处于0和1在不同概率下的叠加态上，就具备了同时存储多个连续值的能力，即模拟电路的特性。所以量子计算机与经典计算机的设计思路迥异，具有非常大的计算潜力。

考虑一个N个物理比特的存储器，若它是经典存储器，则它只能存储2N个可能数据当中的任一个；若它是量子存储器，则它可以同时存储2N个数，因为量子叠加的原理使之可用2N个复系数就能表达出这些数字。例如一个250量子比特的存储器可能存储的数达2250,比现有已知的宇宙中全部原子数目还要多。而且，由于数学操作可以同时对存储器中全部的数据进行，因此，量子计算机在实施一次的运算中可以同时对2N个输入数进行数学运算。其效果相当于经典计算机要重复实施2N次操作，或者采用2N个不同处理器实行并行操作。可见，量子计算机相当于提供了一个天然的并行运算，可以节省大量的运算资源。当量子比特数量增加到N个时，它的存储和计算能力比经典计算机有了指数级提升，达到2N。“量子霸权”（quantum supremacy）一词应运而生[1]。

量子计算机拥有远远超乎经典计算机的计算能力，现在用经典计算机难以破解的加密算法都会被轻易破解。非常著名的一个难题就是大数的质因数分解，据我国量子技术的领军人物潘建伟院士介绍，利用一台万亿次的经典计算机对一个300位的整数进行质因数，需耗时大约15万年，量子计算机上大致只需1秒钟。

但是，量子计算机并不是为了替代经典计算机，二者有不同的用处，犹如火箭飞机不能替代汽车自行车，各有所长。它的用处在于解决一些经典计算机不能解决的特殊问题，比如复杂微观系统的模拟。BCG在一份研究报告中，提出了相比于经典计算，量子计算有以下三类速度优势，不同类型任务的优势大小不一样。

1、显著的速度优势

当用于化学相关研发时，速度优势非常显著。目前，对于分子间相互作用的模拟计算复杂程度随着分子数目的增加呈指数性增长，就跟求大数因数分解似的。量子处理器可以一次性考虑所有的可能交互，并求解最低能量状态，即对应实际的分子交互模式。基于此，BCG预测2030年的，在制药行业，量子计算市场规模将达200亿美元，化学、材料科学等科技密集型产业的规模将达70亿美元。

2、温和的速度优势

面向非结构化的搜索任务，包括一些机器学习的应用，运算时间也会随着问题规模指数性增长。此时，量子算法的优势就体现出来了。有一个经典算法——Grover搜索，利用量子态的纠缠特性和量子并行计算原理，运算时间仅随着问题规模线性增长。

今天，大规模的搜索和机器学习问题是通过大量的、并行的、专门的GPU来解决的。BCG预测，

到2030年，此类取代基于GPU的算法应用规模将超200亿美元。

3、富有潜力的速度优势

当前的经典计算在解决物流优化等复杂操作网络问题时已经显现了良好的性能。根据调研，基于现有算法的可用性，企业认为暂无必要用量子计算替换经典计算。尽管如此，量子计算具有独特的速度优势，当此类问题规模达到一定程度时，量子计算依然有其价值潜力。

量子计算的技术难点

量子计算目前处于基础研究和原型开发阶段，甚至在基础的物理研究上尚未有本质突破。量子计算的技术难点主要有如下三点：

第一，操作和控制量子很难。量子相干和测量的特征决定了制造量子计算机的第一步——操控单量子，实现单个原子、光子的非破坏测量与控制，就是很大的难点。何况，量子计算机若要进入商业化，必须提高量子比特的数量，但量子纠缠的特性使量子数目提高后的操控难度加大，出错概率上升。目前科学家发明了若干种可控的量子系统，最领先的量子计算实验系统只有两种——一个是离子阱，另一个是超导量子电路。其中超导量子电路被视为最有希望的硬件平台。它是一套可以在宏观尺度上对光子和原子进行相互控制和测量的“人造工具箱”。它的各种参数和性质不是由大自然设定，而是可以通过设计在很大范围内进行调整，让科学家可以通过工程方法解决各种实验问题。

第二，观察和测量量子的极端困难性。人们要观察和测量量子，才能用它来制造计算机。但是，要观察和操作量子，必然会使之与环境互动。量子在与环境互动过程中会失去量子的纯正特性，发生“退相干”。量子退相干的时间就是“相干时间”（coherence time），目前所以最好的超导人造原子相干时间只能维持10到100微秒，所以量子计算机最多只能连续工作万分之一秒。

第三，量子纠错是目前最大的瓶颈。为了克服量子退相干丢失信息的问题，我们会想到纠错。纠错在经典信息技术中就很常见，对信息复制多个副本来防止个别副本的错误。在经典计算机中，信息能够在不同的计算机甚至不同文件夹中能够复制，能够在内存中读写。但是量子具有不可复制的特性（no-cloning principle），因为复制之前需要量子观测，这会改变量子的特性。于是人们发明了量子纠错技术（quantum error correction），把一量子比特信息分散存储在几个高度纠缠的量子比特里。单独的天然或人造原子称为物理量子比特（physical qubit），人们通过集成多个冗余的物理量子比特和“量子门操作”（quantum gate operation）形成容错的

逻辑量子比特（fault-tolerant logical qubit），定期地测度这些额外的物理量子比特，发现错误征状来查错纠错。经过量子纠错，逻辑量子比特的寿命会远超过物理量子比特的相干时间，这才是真正能实用的量子比特。不过，量子纠错会产生大量的资源消耗，因为一个逻辑量子比特需要多个物理量子比特以及逻辑操作时的门电路，所以尽量降低资源消耗和错误概率成为量子纠错算法领域的重要研究问题，但仍然比较困难。到目前，任何实验系统都没能做出逻辑量子比特。没有量子纠错的“量子计算机”就只能在相干时间内做一些最简单的运算。Google、IBM等公司近两年一直在比拼芯片上“量子比特”的数量，但其实只是寿命几十微秒的物理量子比特，逻辑量子比特的数量都是零。研究者们退而求其次，发明了“量子错误减少”（quantum error mitigation）策略，较为温和地减少量子计算的错误率，支持简单计算，延长退相干时间。

技术现状和市场未来

1、技术现状和趋势

正如上一节所述，量子技术的难度非常大，图 1 是Science 杂志上的“量子计算难度台阶图”。下一层实验是上一层实验的基础，但这并不是一个直线升级过程——为了上一个新台阶，在它之下的所有台阶都必须不断优化。所以，台阶越高，工作量就越大，量子计算机难度倍增。**目前世界上的所有研究还停留在第三层以下，尚未突破第四层。**

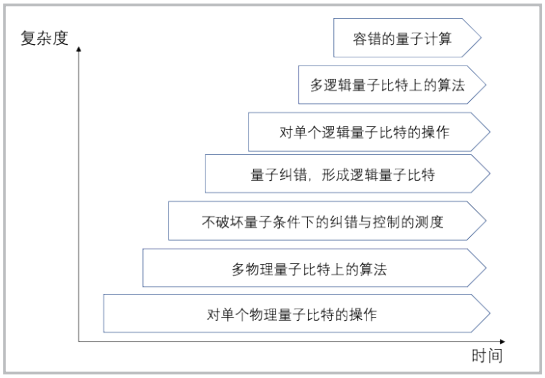


图 1：量子计算难度台阶图

图片来源：M. H. Devoret and R. J. Schoelkopf. 2013. Superconducting Circuits for Quantum Information: An Outlook. Science 339, 1169. 笔者绘制

Gartner在2018年新兴技术热度图中，量子计算正处于创新点燃的爬坡期，受到较为狂热的关注度。但Gartner指出，量子计算距离商业化至少还有5-10年时间。同样地，美国国家科学工程和医学院在近日的一份重要报告《量子计算的进展和未来》中[2]，明确提炼出一个重要观点：“鉴于量子计算的现状和最近取得进展的速度，在未来十年内制造出能够破解RSA2048或类似的基于离散对数的公钥加密系统的量子计算机是非常意外的事。”该报告声称：“如果计算足够可靠以支持大规模环境下的纠错，如今较庞大的量子设备中量子比特的平均错误率需要降低至十分之一或百分之一；在这样的错误率下，这些设备所拥有的物理量子比特数量就需要至少增

加10万倍，那样才能制造出实用数量的有效逻辑量子比特。”

2、市场规模预测

尽管技术达到比较成熟的商业化至少需要10年时间，但量子计算作为一项备受关注的重要新兴技术，被Gartner列为“2019年Top 10 战略技术”之一，业界对于量子计算的商业化路径和市场空间进行了多种预测。

（1）IDC预测

知名的信息技术、电信行业和消费科技咨询公司IDC认为，量子计算商业化的过渡路径是将量子和古典计算结合成一个“混合量子/古典”层来加速计算，应用程序可以通过API选择量子计算（或传统计算）作为计算层。这种方法使应用程序能够分时共享基于云的量子计算资源，这些资源由公共云服务提供商提供。在商业化早期，该异构解决方案将成为标准的应用模式。在该异构方案基础上，IDC提出了量子计算三步走的预测：第一，现有的工作负载随着时间推移而转移到混合量子计算，并最终成为量子计算的用例。第二，全新的基于量子计算的工作负载，这些工作负载只能在量子计算机上运行。第三，到2027年大多数云计算的应用程序将转变为量子优先的用例，在处理超出传统计算机处理能力的数据集时，会自动调用量子代码，与此同时这样的应用程序将在许多中大型企业中运行，用来解决一些新的计算问题。IDC预测，2027年时全球的量子计算规模将比现在高出40倍，市场空间将达到107亿美元。

（2）BCG预测

BCG认为，量子计算要进入商业化运作，至少要让逻辑量子比特达到一定数量。2017年底，已经有研究人员以99.9%的逻辑成功率实现了14个量子比特的纠缠。量子模拟大约需要150个逻辑量子比特，每一个逻辑量子比特都由10到数千个物理量子比特组成。为了达到这一步，它与IDC一样，预计需要“三步走”，只是这个“三步走”要经过未来25年的发展。

在第一阶段(2018年-2028年)，工程师们将开发非通用量子计算机，用于低复杂性模拟等应用。这些计算机的大部分开发将在未来几年进行，它们将一直使用到第二代到来之前。第二阶段(2028年-2039年)将是量子计算机扩展到50个逻辑量子比特并在经典计算的基础上取得“量子优势”的时期——这意味着它们将能够在特定的应用中更快地执行某些算法。第二代量子计算将集中在分子模拟、研发和软件开发等问题上。在此期间，可用的应用程序将进入市场，创造重大价值。与此同时，量子信息处理作为一个领域将会进一步发展，企业将会更加熟悉量子模拟的方法。在第三阶段(2031年-2042年)中，量子计算机将在高级模拟、搜索和优化的商业应用取得比经典方法更有显著优势的规模。总体看来，BCG预计量子计算将在未来十年稳步发展，到2030年左右将出现显著加速发展。

BCG预测，假设量子纠错技术的发展速度按照摩尔定律前进，并且技术遵循S型曲线，那么**该基准情景下的量子计算应用市场在2035年将达到20亿美元左右；到2050年，随着应用的增多，市场将飙升至2600亿美元以上。**如果在乐观情景下，量子纠错技术的发展很快，那么2030年在制药行业，量子计算市场规模将达200亿美元，化学、材料科学等科技密集型产业的规模将达70亿美元；2035年的市场规模约为600亿美元，到2050年将增长至2950亿美元。

如果仅看近10年情况，BCG在另一份研究报告中预测[3]，2022年前，学术界的量子计算市场年增长率为44.8%，政府为46.5%；从2022年到2027年，企业应用市场被打开，其中金融界会以72.4%的年增长率进入到这个市场，还有化工界（增长率72.4%）和能源界（增长率64.9%）。按应用领域分，从2022年到2027年，金融分析市场的年增长率为62.6%，随后是广告和机器学习。2027年，整个市场将达到13亿美元。

(3) 其他预测

除了IDC和BCG之外，也有若干家机构预测了量子计算的未来市场。Tratica预测，2025年的全球市场规模将达到22亿美元；Market Research Future预测，2022年就是2.5亿美元；Persistence Market Research预测，2025年的全球市场规模为230亿美元，年复合增长率是30.9%；著名统计机构Statistica则大胆预测2024年的市场规模则将达107亿美元，其中企业界贡献84.5亿美元，而政府的科研资助金额将达到22.5亿美元。

各家机构对量子计算的市场空间规模、时间点的预测相差迥异。其中BCG的基准情景预测是基于摩尔定律推算。美国国家科学院的报告指出，量子世界是否适用于摩尔定律还有待观测，因为摩尔定律本质上是生产、投资正向反馈下的加速学习曲线，如果量子计算无法呈现出正向反馈的加速学习，那么就无法达到摩尔定律。

因此，BCG的基准情景预测虽然在各种预测中最为悲观，但相对谨慎可靠。综合而言，**十年后即2030年左右，全球量子计算市场规模至少达到20亿美元，最乐观情境下达到200亿美元。市场规模年增长率至少在20%以上，并持续到将近2050年。**

量子计算的应用价值

作为具有超强计算能力的未来计算机，量子计算在多种计算场景上能发挥独特的应用，并在多个垂直行业中体现应用的价值。下图 3从计算问题和垂直行业两个视角构建了量子计算的应用矩阵。可以看到，量子计算适用于优化、仿真、传感测量、密码学、人工智能等多个计算场景，从而适用于金融、化工、材料、医疗、制药、通讯、能源、基础物理和计算机科学等多个不同的垂直行业需要。

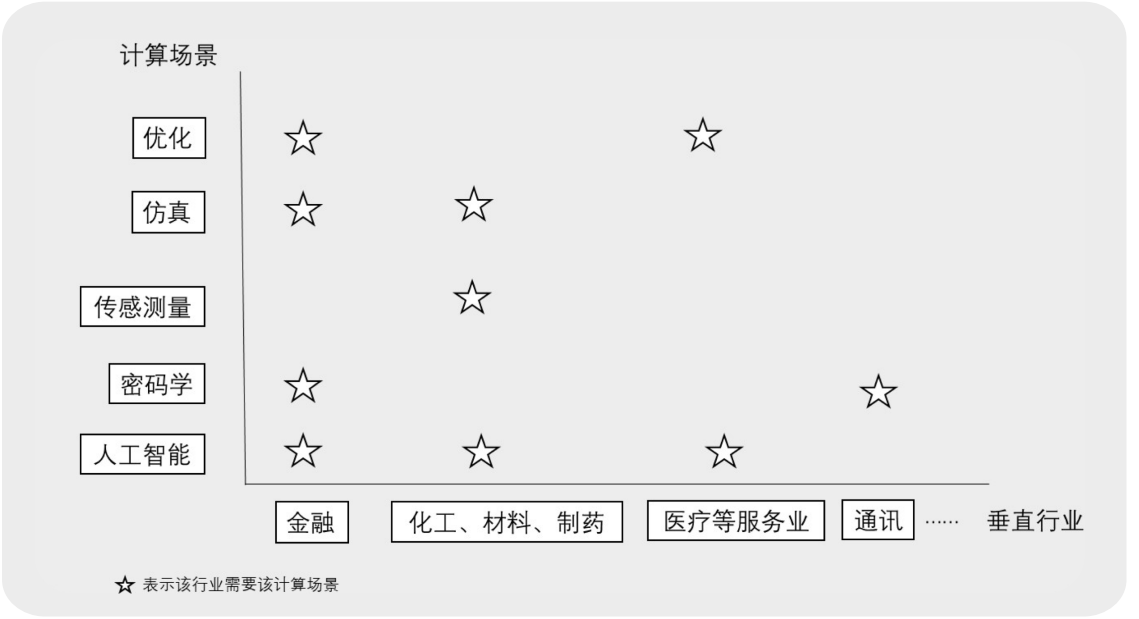


图 3：量子计算的应用矩阵

计算场景

1)量子优化（quantum-assisted optimization）

运筹学、物理学、社会科学以及各个行业中所有涉及量化计算的一个核心与困难的计算任务是优化。这些问题往往有指数级的计算复杂度（业内术语称为NP-hard），经典计算机的计算速度太慢。想象一个由成千上万个由桥梁连接起来的群岛，需要找到一条只穿过每个岛屿一次的道路（即所谓的“一笔画”问题）。可能的解决方案的数量随着岛屿的数量呈指数级增长。如果我们假想的岛屿难题有100万种可能的解决方案，那么一台经典计算机平均需要50万次尝试才能找到合适的解决方案。运行量子搜索特定的Grover算法，需1000次就能解决问题——速度快500倍。短期内，人们可以开发将量子计算和经典计算机混合的“量子近似优化算法”（quantum approximate optimization algorithm），经典计算机来指挥量子处理器如何排布量子比特，量子处理器来具体解决优化。

2)量子仿真（quantum simulation）

经典计算机在仿真模拟高度动态复杂的问题时会出现很大困难，例如对环境参数变动高度灵敏的天气预报系统。对于微观粒子的运动模拟，经典计算机更是捉襟见肘。而量子计算机则具

有很大优势来仿真量子力学。

3)量子传感测量(quantum sensing)

量子技术对于某些传感测量问题具有很好的优势,由于量子不可测原理,它能侦测到极度轻微的力的变化,因此比其他传感技术具有更高的灵敏度和分辨率。

4)量子密码学(quantum cryptography)

由于量子计算机惊人的计算能力,它对能抵御经典计算机的当前公钥密码体系具有极强的破坏力。经典的非对称加密体系运用RCA算法、ECC椭圆曲线算法等来创建公私钥,但这些算法根基在于大数字的质因数分解、离散对数等数学难题上。常规计算机对这些难题的解决能力很弱,但量子算法例如Shor算法能够将指数级运算时间降低到多项式级,Grover算法也可将O(N)级时间降到开方级,大大加快了运算时间。有估计,2027年量子计算能够在10分钟左右破解加密签名。哈希加密的信息同样很可能会在很短时间内得到破解。为了解决潜在的威胁,密码技术同样在不断改进,人们正在研发改进新的加密技术,即“抗量子的加密技术”(quantum-resistant cryptography)。

5)量子计算与人工智能

以机器学习、深度学习为主要技术代表的人工智能是量子计算应用的另一大重要场合,是量子优化和仿真技术在特定领域的延伸。搜索算法以及基于机器学习的大型多层神经网络需要在大型数据集以及通过反复试验和监督学习获得大量结果的基础上进行训练。虽然机器学习和人工智能已经通过大型数据集和并行、低成本GPU、专用AI芯片的结合成为现实,但量子计算机可以加速神经网络的训练,并增加它们能够处理的数据量。该项应用是一个活跃的研究领域,因为科学家和工程师试图识别可以用于解决机器学习的量子算法。BCG预测,量子计算机相对于传统计算机的基本优势可能导致到2030年时有200亿美元的高性能机器学习计算市场将被取代。不过,也有专家认为,量子计算机用于深度学习的优势并不一定有想象中的那么大[4]。量子计算的优势在于将在经典计算机下的大量经典数据(classical data)以非常简洁的形式表达出来,例如将一个N维向量用logN个量子比特即可表达,但真正的瓶颈在于大量经典数据编码存入量子网络或读取出来时的成本太大,因为量子状态数据和经典状态数据的转换有损耗。因此,量子深度学习更有优势的场景应该是输入输出数据都是量子态,处于不确定概率分布的时候。量子深度学习的元件并不一定要用在一般功能的量子计算器上,更适合作为一个特殊的器件。

垂直行业

化工、材料和制药行业是量子计算最先可能商用的垂直行业。无论是飞机制造需要的更强的聚合物、用于汽车的更有效的催化转换器、更高效的太阳能电池材料，还是疗效更好的药物或透气性更好的织物，更快的开发速度都将带来巨大的价值。模拟化学反应和材料、建立计算机模型是最值得期待的量子计算实际应用之一。从定性描述到定量预测，量子计算机都将对计算机材料模拟和发明带来根本性的变化，因为量子计算机显著的速度优势在于用来了解特定的相互作用和化学过程的大型分子建模。

化学反应率对分子能量非常敏感，其跨度范围远远超出传统计算机的处理能力。开发出稳健的量子算法，就有可能完成一些重要材料的仿真任务。不需要花费数年时间，也不需要数亿美元的投入，研究人员可以使用量子处理器来创建一个量子孪生仿真模型（quantum twin），通过量子计算机仿真对数以百万计的候选方案进行研究，开发出少量新材料并确定其性能。制药和化学公司已经在试验量子模拟的潜力，以加速药物的发现和减少设计分子的意外副作用。这些行业的高管估计，以这种方式识别新目标，可以将药物发现率提高5%至10%，并将开发速度提高15%至20%。BCG报告指出，仅在美国的制药行业，如果今天能提供处理复杂原子的量子仿真，将会有10%的公司愿意为此功能付费，量子计算将提供150亿到300亿美元的市场机遇。

通讯业是量子通信和量子计算交叉应用的重要领域。量子通信的基本原理是量子测量。最经典的方式是通过量子通道传输密钥，即量子密钥分发（Quantum Key Distribution, QKD）技术。在通信过程中，加密信息的密钥通过专用的量子通道进行传输，用量子比特作为密钥。由于量子测量的原理，观察或者测量一个量子系统均会造成量子比特的扰动，改变状态，造成检测反常，就会提醒通信双方泄密，窃听者本人也很难获得真实量子信息。相比经典通信，量子通信还有时效性高、传输速度快、抗干扰能力强、跨多种媒介等优点。除了QKD外，另一个应用设想不是分发密钥，而是直接将数据嵌入到用量子流（Quantum Stream）中，让窃听者难以获得真实信息。除了量子通信技术外，量子计算在通讯业中的最直接应用则是对加密系统的重大威胁，上一节已经说明了这个问题。

需要优化计算的垂直服务行业，如医疗、电力、物流交通、零售等，也有量子计算的用武之地。建立在量子计算和传统计算机组合基础上的量子近似优化算法解决方案非常强大，可在许多行业中用于提高产品质量和服务质量。例如使用优化算法实施广告的在线推荐和报价策略，以最有效的方式应对消费者的需求和市场变化；物流公司可以优化调度、规划和产品分配。量子算法还可用以提

高病人医疗诊断的速度和准确性，人们可以在数秒内完成DNA排序、放射疗法优化、脑肿瘤诊断等以往需要数小时乃至数周才能完成的任务。

量子计算遇上金融业：双刃剑

作为非常重要的一门服务业，金融行业同样面临着大量优化、智能化、加密等计算问题，同样需要处理海量数据，因此量子计算也有很大用途，但也具有很大潜在威胁，是一把双刃剑。

第一，量子计算能够大大提高金融机构在处理高频交易、对冲、定价等方面的能力。面对高度波动的证券市场和海量信息，高频交易比拼的一个关键就是运算速度和信息处理能力。量子计算显然比传统计算机具有更大的优势。此外，金融机构在对冲策略、定价策略上需要优化模型时，量子计算在优化算法上的巨大求解能力也有助于模型的提升和应用。

第二，量子计算加速机器学习，从而提高人工智能在金融行业的众多应用能力。不论是反洗钱、客户识别、信贷风控、智能客服、智能投研等哪一个场景，基于机器学习的人工智能都具有重要的应用，这些场景的金融智能化是大势所趋。量子计算能显著有效加速大规模神经网络中的深度学习，拓展其数据处理速度和处理量，从而进一步提高金融智能化水平。

第三，量子计算能显著增强金融区块链的并发能力。制约区块链发展的一个重要瓶颈是出块速度不高，并发量低，这使得区块链应用于需要高并发的大规模金融支付清算业务时捉襟见肘。系统运用量子计算加快签名验证、Hash码验证、Merkle树搜索等所有计算任务后，能有效提高吞吐量，使金融区块链的应用更加便捷。

第四，量子计算能有效拓展金融云的处理能力。未来的云计算可以采用量子计算和经典计算混合的异构方案，当经典计算服务无法满足资源调度和云上数据处理需求时，量子计算服务就被启动，在短时间内重新优化调度云服务资源，并满足数据计算需求。这样，在当前云服务上消耗巨大资源的高性能计算任务，如超大规模神经网络训练、类脑计算等，就能被轻易承载，这样金融云的作用就能得到极大增强。

第五，量子计算也有很大负面威胁，特别是对现有加密算法的威胁，因此对金融安全以及金融区块链应用提出了严峻挑战。正如上两节所述，量子计算能轻易破解现有RSA、ECC等加密算法体系，对当前银行加密技术体系中的非对称密码体系、Hash算法会产生很大威胁，金融区块链也失去了安全。现在几乎所有金融公司都有两个共同的缺陷——依赖于现有硬件、很难在短时间内修改加密标准，所以给量子解密的黑客攻击留下了想象空间。尽管量子计算在十年内还很难商用，但这个威确实存在，需要提早谋划，进行量子风险评估，以确定与其当前加密基础设施相关的风险。

量子计算应用于金融科技的市场和效益

技术效益

量子计算将与机器学习、区块链、云服务、大数据处理有效结合，随着业务多样性增多、复杂度增强、要求的计算能力越来越高时，量子计算的商业效益将愈发明显：

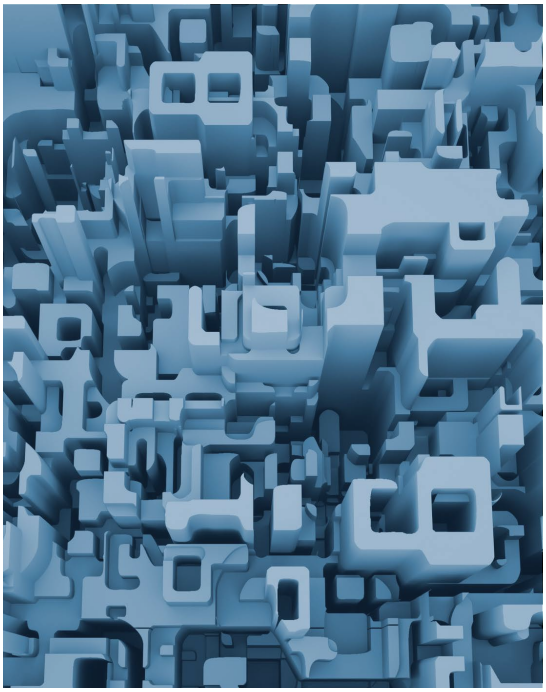
1)AI（机器学习）：量子计算机的机器学习可以帮助我们更快、更高效地做很多事情，具体应用场景包括人脸识别、图像理解、音频语音理解、用户画像等，量子算法的研究可能给未来AI算法带来全新的思路，基于量子硬件的机器学习算法，可以加速优化算法和提高优化效果。

2)Blockchain（区块链）：当节点应用量子计算后，能够极大提升Hash码验证、签名验证等计算速度，从而增强金融区块链吞吐量，使区块链技术的应用基础更加牢固。

3)Cloud Computing（云计算）：量子计算能有效拓展金融云的处理能力，量子计算提供的是大规模并行处理，原子级存储和试用物理定律而不是外部加密的安全，未来的云计算可以采用量子计算和经典计算混合的异构方案，金融云的作用能得到极大增强。在云上架构量子处理器就是一个很好的方向。

4)Big Data（大数据）：量子计算与大数据处理一开始结合的点可能是先针对当前一些计算密集型、对算力要求高，但算法又比较单纯的场景，比如数据传输、存储的加密，压缩，把量子计算作为一种计算加速服务。

此外，提前布局开发抵抗量子计算机攻击的新型加密算法和方法（“后量子密码学”）能提升金融行业的数据安全性，防止攻击。根据美国国家安全局信息保障司（IAD）要求，美国的国家安全系统算法至少要能够保障信息安全达30年，届时能否抵抗量子计算机尚不得而知。所以国会于2017年制定“美国创新与竞争力法案”（The American Innovation and Competitiveness Act），责成国家标准与技术研究院（National Institute of Standards and Technology, NIST）研发抗量子密码算法。目前QRC算法可分为基于编码的算法（Code-based Encryption，C类）、基于多变量多项式的加密算法（Multi-variable Polynomial，M类）、基于安全散列函数的算法（Secure Hash-based，S类），以及基于格栅的加密算法（Lattice-based Encryption，L类）等，L类最有名的代表就是现在热门的全同态加密。这些算法正在尽快研究与标准化过程中，如果从业者能够尽快参与到这个过程中，对区块链和量子计算两大领域的探索将有很大的潜在价值。



商业效益

量子计算市场规模十年后即2030年左右，全球量子计算市场规模至少达到20亿美元，最乐观情境下达到200亿美元。市场规模年增长率至少在20%以上，并持续到将近2050年。因此提早进入量子计算的布局并做好长期规划，有利于与“ABCD”等其他技术相结合，进一步巩固金融科技领先优势，获得量子市场的市场份额。

2030年，中性情景的全球市场规模约为100亿美元，假设中国市场占据全球10%，即10亿美元，如2.4节援引BCG报告所述，虽然化工医药材料是最重要的应用部门，但金融分析是增长最快的细分市场，假设金融分析占据了20%的规模，则规模为2亿美元。**在提早布局、占据先机和行业影响力的情况下，金融科技企业有望与合作伙伴共同分享2亿美元的市场空间。**

风险评估

布局量子计算技术，可能存在主要三大风险，相应的防范对策如下：

1)技术风险

距量子计算进入实用可能还需要一段时间，目前主要的竞争是在学术方面，量子计算可以更迅速地解决目前已知的一些问题，并为解决未来问题提供新的工具，量子计算市场将突破百亿美元，只是时间的问题，技术上商用化的不确定的风险较高。

2)竞争风险

当前，美国、中国、欧盟、英国、荷兰、日本、加拿大、澳大利亚等国家争先布局，美国还将量子技术纳为限制性出口技术，各国希望占领量子技术领域的领先地位，国际上竞争较大，有较大政策风险（如出口限制）；我国科技巨头BAT自2015年开始布局，建立实验室，邀请顶尖学者和科学家作为负责人展开研究，华为、中科院等均有所动作，市场竞争大，需要投入较大的科技研发投入与资金投入，进入门槛高，大科技机构成为市场的主要玩家。

3)资金风险

进行量子计算技术布局需要耗费资金投入和人员投入，如果量子计算商用化进程过慢、与现有业务无法很好结合地应用，效果不达预期，存在资金投入风险。

【注释】

[1] J. Preskill, Quantum computing and the entanglement frontier, 25th Solvay Conference

on Physics (2011),

[2] National Academies of Sciences, Engineering, and Medicine. 2018. Quantum Computing: Progress and Prospects. The National Academies Press, Washington, DC.

[3]https://globenewswire.com/newsrelease/2018/08/09/1549483/0/en/Global-Quantum-Computing-Market-to-See-37-3-Annual-Growth-Through-2022.html

[4] J. Preskill. 2018. Quantum computing in the NISQ era and beyond.

金融科技·微洞察

“金融科技·微洞察”是微众银行运营的金融科技研究品牌，聚焦国内外金融科技领域的技术发展、标准制定及产业应用，把握当下金融科技热点话题与政策动向，洞察未来领先的金融形态和商业模式。

微众银行作为国内首家互联网银行，自2014年成立之初即将“科技、普惠、连接”作为银行的三大发展愿景，将积极运用科技创新探索普惠金融新模式、新业态作为银行重要的发展方向，致力于为普罗大众、微小企业提供差异化、有特色、优质便捷的金融服务。自立行至今，微众银行在金融科技“ABCD”（人工智能、区块链、云计算、大数据）等四大领域积极探索，2017年即已成为国内首家获评“国家级高新技术企业”的商业银行，截至2019年末共申请国家及国际专利数超过1000余件，拥有自身所有重要业务和技术系统的知识产权，有效实现了银行业信息化安全可控的战略目标。2019年，全球最具影响力的独立研究机构之一Forrester在银行案例研究报告中将微众银行定义为“世界领先的数字银行”。

金链盟

深圳市金融区块链发展促进会（简称“金链盟”）成立于2016年5月，由微众银行、腾讯、深圳市金融科技协会、深证通等二十余家金融机构和科技企业共同发起，2019年11月正式注册为社会团体法人。至今，金链盟成员已涵括银行、证券、基金、保险、地方股权交易所、科技公司等六大类行业的150余家单位，成为国内最大的区块链组织和最具国际影响力的区块链联盟之一。

金链盟开源工作组于2017年推出了安全可控、稳定易用、高性能的金融级区块链底层平台——FISCO BCOS（Be Credible, Open & Secure）。该平台获得了2018年度深圳金融科技创新专项奖一等奖，并于2019年入选成为国家级区块链服务网络（BSN）中的首个国产联盟链底层平台。目前，FISCO BCOS开源生态圈已汇聚了上万名个人开发者、超1000家机构与企业，在政务、金融、公益、版权、供应链、教育等不同领域已有80余个落地应用，发展成为最大最活跃的国产开源联盟链生态圈。

免责声明

在任何情况下，本报告中的信息或所表述的意见并不构成对任何人的投资建议，本报告所载的资料、工具、意见及推测只作参考之用，并非作为或被视为出售或购买证券或其他投资标的邀请或向人作出邀请。在任何情况下，报告的编著机构不对任何人因使用本报告中的任何内容所引致的任何损失负任何责任。

所载资料仅供一般参考用，并非针对任何个人或团体的个别情况而提供。虽然我们已致力提供准确和及时的资料，但我们不能保证这些资料在阁下收取时或日后仍然准确。任何人士不应在没有详细考虑相关的情况及获取适当的专业意见下依据所载资料行事。

关于我们 ABOUT US

联合出品

WeBank 微众银行 | 金融科技 微洞察 FISCO金链盟

报告出品人

姚辉亚

报告统筹

李 斌

报告作者

徐 磊　魏思远

美术编辑

邓少雁

联络邮箱

weinsights@webank.com

金融科技·微洞察