量子计算在经济与金融领域中的应用*

汪 勇　孟香君　沈维萍

摘要：近年来量子计算快速发展，以其运算速度远超超级计算机而著称，受到社会各界的广泛关注，并在经济与金融领域产生了重要影响。本文就量子计算的发展现状、基本原理及其在经济与金融领域的应用进行系统梳理。本文发现，量子计算的高效率能有效提升经济预测效果、改进期权定价、优化投资组合的选择、改善商业银行的信用评分与风控模型，但也会对数字货币带来一定的安全隐患。在此基础上，本文深入分析了量子计算优化经济与金融运行的内在机理，并探讨了量子计算威胁经济与金融发展的潜在机制。最后，本文总结讨论了量子计算促进经济与金融发展的方向以及未来量子计算技术发展和应用存在的潜在挑战。

关键词：量子计算　经济预测　期权定价　投资组合　数字货币

近年来，量子科技作为新一轮科技革命和产业变革的前沿领域获得快速发展。各国在该领域展开角逐，加紧布局以抢占先机。美国、欧盟、俄罗斯、日本等世界主要国家和地区通过出台政策文件、成立研究机构、支持量子科技研究等方式加大对量子科技的支持力度，我国也将量子科技产业作为国家战略来大力支持，2016 年在国务院《国家创新驱动发展战略纲要》中提出了促进“量子信息技术”发展的战略规划。2020 年 10 月，习近平总书记在中央政治局第二十四次集体学习时强调，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，抢占量子科技国际竞争制高点。

当前，各大知名企业、高校、科研机构等使用不同的核心技术构建量子系统。一方面，量子计算能够比现有的经典二进制算法更快地解决某些问题。一旦克服了当前的技术障碍构建出一台功能齐全的通用量子计算机，将会彻底改变需要强大计算能力来进行模拟和优化的领域，经济与金融领域就是其中之一。现代经济与金融发展面临着很多具有挑战性的计算问题，比如使用蒙特卡洛方法进行期权定价、使用随机微分方程对金融市场建模、优化投资组合、使用机器学习技术进行分类与预测等，量子计算的出现可以大幅缩短模拟和优化的时间，提高经济与金融模型的准确性，加速经济与金融领域的智能化。另一方面，量子计算的高效计算能力也会给经济与金融发展带来新的风险与挑战。例如，常见的 ATM 交易、数字货币以及互联网中的密码算法在量子计算面前不堪一击。金融机构和监管机构等需要重视量子计算的风险，对现有密码体系进行升级，并尽快探索量子密码学在经济与金融加密中的应用。本文旨在梳理量子计算在经济与金融领域中的应用与最新研究进展。

一、量子计算概述

（一）量子计算的概念与发展脉络

1. 量子计算的概念。量子计算作为新一轮的科技前沿领域，目前仍然处于发展的初期阶段。1900 年，普朗克在对热辐射的研究中提出了能量量子化假说（Planck，1901）。该假说认为能量值只

* 汪勇，中国社会科学院金融研究所，邮政编码：100710；孟香君（通讯作者），中国社会科学院大学，邮政编码：102488，电子邮箱：mengxiangjun0123@163.com；沈维萍，华夏银行博士后科研工作站/中国社会科学院金融研究所博士后科研流动站，邮政编码：100027，电子邮箱：swpjiayou@126.com。基金项目：国家社会科学基金青年项目“银行数字化转型与货币政策传导有效性研究”（21CJY066）；中国社会科学院青年科研启动项目“低碳生活与家庭资产配置”（2022YQNQD036）。感谢匿名审稿专家的宝贵意见，文责自负。

能取某个最小能量元的整数倍,这一最小能量元即为“量子”。经过爱因斯坦、玻尔、德布罗意、海森伯、薛定谔、狄拉克、玻恩等人的完善与发展,于20世纪20年代中期形成了完整的量子力学理论体系。20世纪70年代,控制单量子系统的技术得到发展,对将量子力学应用于量子计算和量子信息研究起到根本作用。20世纪80年代初,Benioff(1980)首先提出了量子计算的思想。

量子计算是指利用叠加和纠缠等量子现象来进行计算(Deodoro et al, 2021)。经典二进制计算机最小的存储单位是比特(bit),比特的取值有“0”和“1”两种。量子计算机最小的存储单位是量子比特(qubit),也称量子位,量子比特的取值可以是“0”、“1”,也可以是“0”和“1”叠加的状态,也即一个量子比特可以表示“0”和“1”两个值按照任意比例叠加的状态。对经典计算机而言,n个比特能够表示包含“0”或“1”的2^n种组合,而n个量子比特却能够表示2^n个叠加状态。随着n的增加,量子比特储存的信息量将以指数的形式上升,存储信息的能力远超经典比特。经典计算机只能对2^n个数中的一个进行数学运算,而量子计算机的每一步都可以对2^n个数据同时做出酉变换(幺正演化),实现高速并行运算,一次运算相当于经典计算机进行2^n次运算,处理信息的能力远超经典计算机。

1981年计算物理第一次会议对量子计算达成了共识:量子计算机将信息存储在量子比特中,并且可以利用量子纠缠和量子干涉原理来解决指数级大数据计算的问题。理论上,当量子计算机达到50量子比特时,它对特定问题或特定实验环境的模拟与计算能力就能远超现有的超级计算机。只有几百个量子比特的量子计算机所执行的计算量,要比已知宇宙中的原子数量更大。然而,量子计算机只会在对计算数据量大的问题上超过经典计算机。对于普通的计算量小的加减乘除等算法,经典计算机计算速度方面已经满足了正常需求,量子计算机在这些问题上没有优势。因此,量子计算机不可能完全取代经典计算机,只能在某些有特定难度的问题上替代经典计算机,实现量子加速。

2.量子计算的发展脉络。在Benioff(1980)提出量子计算思想的基础上,美国物理学家Feynman(1982)提出了按照量子力学规律工作的计算机的概念,并预见到量子计算机相比经典计算机更适合用来模拟量子物理系统的特性。Deutsch(1985)提出了量子图灵机模型。美国物理学家Shor(1997)提出了著名的量子算法,证明量子计算机可以高效地解决大数分解问题,并可能破解广泛使用的RSA公共密钥体系,引发了全世界广泛的关注。2007年,加拿大D-Wave公司率先推动量子计算机的商业化,成功研制出一台具有16量子比特的“猎户星座”量子计算机,2011年又研发了全球首台基于量子退火的商用量子计算机,2015年和2017年又先后推出了1000量子比特和2000量子比特的量子退火机。2017年IBM推出了一台50量子比特的计算机,随后在2019年发布了全球首台独立商用量子计算机。2018年谷歌公司研制一台72量子比特的通用量子计算机。2020年12月4日,中国科学技术大学的潘建伟等人成功构建76个光子的量子计算原型机“九章”,求解数学算法高斯玻色取样只需200秒,而目前世界最快的超级计算机要用6亿年,这一突破使中国成为全球第二个实现“量子优越性”也即“量子霸权”(Preskill, 2011)的国家。在当前世界各国量子计算的竞赛中,美国处于明显领先地位,形成了政产学研多方协同的良好局面。谷歌、IBM、英特尔等科技巨头投入数千万美元,与耶鲁大学、麻省理工学院等知名高校开展合作,在量子计算领域取得了较好成果。近年来,我国也不断加大对量子计算研发的投入,并在相关领域取得了一定的成果。2018年,阿里云与中科院成功研发11量子比特计算云服务系统,同年华为发布量子计算模拟器HiQ云服务平台。国内首家量子计算公司合肥本源量子计算科技有限公司于2017年成立,同年发布了一个32位量子计算虚拟系统,同时还建立了以该系统为基础的本源量子云计算平台。

虽然量子计算机在理论上是可行的,但是通用量子计算机目前仍然面临技术困难,当前对量子计算机硬件的研制还处于初级阶段,已有的一些硬件都有一定的局限性,要想真正取代超级计算机进入实用阶段,还需要在实验和理论上都有所突破。在达成通用量子计算这一长远目标之前,一个阶段性的里程碑就是量子计算的优越性,也即到达经典计算机无法做到的事情的关键节点。在现阶段以高校院所开展量子计算系统实验室研究为主,中期逐步过渡到以公司为主开发实用模拟机器件,以企业化方式推动实用器件开发替代技术验证机,但成熟产品及民用推广还需时日。通用的量子计算机面世时间难以预料,科学家依然面临着严峻的挑战。但在中长期,作为未来技术的发展趋

势，量子计算的商业应用前景较为乐观，将在对计算需求量大的领域带来革命性进步。

（二）量子计算的原理与算法

经典的二进制计算机内部采用布尔运算操作比特，输出结果为数字，量子计算机输入量子比特，计算机内部对量子比特进行模拟操作，输出结果需要进行专门的测量才能得到。量子计算可以在离子、光子或者微小的超导电路中实现。中国科学技术大学于 2020 年 12 月构建的量子计算原型机“九章”就是用光子实现的，它依靠激光束进入反射镜和透镜组成的阵列进行信息处理，以光子代替电子，光运算代替电运算。

量子空间进行模拟操作运用了量子纠缠原理。制备一种几个粒子共同的量子态，称为量子纠缠态。当一个粒子发生改变时，其他粒子并没有受到干扰，没有受到相互作用的影响，但是它的状态却受到关联关系的制约，已经发生了变化，即无法单独描述各个粒子的性质。量子纠缠现象违反了经典物理学理论，这种特性是使得量子的运算能力成指数型增长的根本原因，可以用于量子计算机、量子保密系统以及量子通信等领域。

量子比特对环境较为敏感，一个极其微小的相互作用都会让其发生改变。环境中有许多粒子，每个粒子都在不同的方向上随机运动，由此产生了噪声。噪声的存在使得储存在设备中的数据产生波动，最终使得计算结果出现误差，大大削弱量子计算机的计算能力。减少噪声带来的影响的过程称为量子纠错。量子纠错也是量子计算的一个重要部分，要想建立一个实用的量子计算机，必须能够减少噪声、控制大量的量子比特。量子纠错采用奇偶校验方法，但是量子力学中的不可克隆定理（no-cloning theorem）（Wootters & Zurek，1982；Dieks，1982）决定了不能简单直接将经典纠错码转换成量子纠错码。量子纠错通过引入大量的辅助量子比特，与原有的量子比特发生量子纠缠，其后再像经典比特中的奇偶校验一样测量辅助量子比特。这样，尽管测量辅助量子比特导致了其量子态的塌缩，但是并没有对原有的编码比特产生影响，即原有的信息并没有发生改变（Gottesman，1997；Aharonov & Ben-Or，1997；Campbell et al，2017）。

第一种量子算法由 Deutsch（1985）提出，用于判断从 Z_2 到自身的函数是否为常值函数的问题。传统的计算方法需要调用函数两次，而由于量子比特的叠加特性，Deutsch 算法只需调用函数一次。Deutsch & Jozsa（1992）进一步将这个算法拓展到了判断 Z_2^n 到 Z_2 的函数。Simon（1997）提出了一个量子算法来解决他自己设计的一个计算问题，这个算法比 Deutsch-Jozsa 算法更能证明量子计算的优越性。受此启发，Shor（1997）提出了著名的 Shor 算法，从而对量子计算领域产生了巨大的影响。Shor 算法可用于大数因子分解，比目前传统最高效的经典质因数分解算法快了一个指数级。Shor 算法最重要的一步是使用了量子傅里叶变换 QFT（quantum Fourier transformation）（Gamache et al，1983），量子傅里叶变换能够通过量子纠缠、量子态叠加等实现高效的傅里叶变换，时间复杂度为 $O(\lg(N))$。Shor 算法是一种随机算法，不能保证每次运行都得到正确的结果，通常通过增加实验次数来提高得到正确结果的可能性。

另一种非常重要的算法是 Grover 算法，它是一种非结构化搜索量子算法（Grover，1996），被认为是继 Shor 算法之后的第二大量子算法。与经典的搜索算法相比，Grover 算法实现了多项式加速。传统的搜索算法需要将 N 个要搜索的数据逐一进行检验，平均需要查找 N/2 次，成功的概率为 1/2，时间复杂度为 $O(N)$。而在 Grover 算法中，可同时验证 N 个值是否是所要查找的数值，时间复杂度为 $O(\sqrt{N})$。Grover 算法得到正确结果的概率最大为 $1-2^{-N}$，当 N 较小时具有一定的失败率，龙桂鲁等（2004）提出了一种成功率 100％的改进 Grover 算法，并发现在 Grover 算法中相位取反操作只能采用满足相位匹配条件的角度替代。Grover 算法作为一个高效的搜索算法应用较为广泛，可以用来求最大值、最小值、平均值等。要搜索的数据库中数据越多，Grover 算法就越显得高效。刘晓楠等（2021）提供了关于 Grover 算法改进与应用的更详细介绍。

线性系统的求解在计算中是一个重要的问题，量子算法求解线性系统比经典算法快得多。Harrow et al（2009）提出了第一个求解稀疏线性系统的量子算法 HHL 算法，时间复杂度达到 $O\left(\frac{\kappa^2(\log M)}{\varepsilon}\right)$，其

中 ε 为精度,Childs et al(2017)的工作进一步降低了 HHL 算法的时间复杂度。Chen & Gao(2022)提出了一种求解布尔多项式系统的量子算法,Chen et al(2018)将该算法推广到有限域上求解多项式方程。

将量子计算应用于神经网络可以使得复杂的神经网络得以训练并实现训练的加速。Kak(1995)首先提出了将量子并行性、量子纠缠等量子计算的特性用于复杂的神经网络训练的量子神经网络(QNNs)的思想。Farhi & Neven(2018)为适用于量子处理器上的监督学习建立了一个通用框架,并进行了模拟,结果表明,在近期门模型(near term gate model)量子计算机上运行该量子神经网络是可能的。相干伊辛机(CIM)是一种混合量子计算平台,与其他基于门的技术路线相比,相干伊辛机更像人的大脑神经突触的工作模式,更能抵御噪声干扰,更加适合于较大的量子神经网络(Yamamoto et al, 2020, Bharti et al, 2021)。

量子退火机是常用的量子设备,依靠的是量子退火算法(QA)(Kadowaki & Nishimori, 1998)。量子退火可以用来寻找离散空间内目标函数的局部最优解,它设计的目的就是在组合优化问题中寻找局部极小值。经典退火使用热力学来寻找极小值,热波动保证了系统在不同局部极小值之间跳跃,当温度降低时,向较差解移动的概率趋于零。在量子退火中,这些跃迁是由量子隧穿效应驱动的,能够更快地穿过局域极值点旁的势垒,这比传统热力学探索局部极小值更有效。

(三)量子计算的优势与面临的挑战

量子计算建立在量子力学规律的基础之上,与传统的计算方法相比具有以下优势:首先,量子计算机的计算能力远超经典计算机。由于量子比特的叠加性和纠缠性等物理性质,对 n 个量子比特的计算机而言,其处理数据的能力是经典计算机的 2^n 倍,能够处理的数据量远超经典计算机。其次,量子算法在处理时间复杂度方面远远优于传统算法,往往有指数加速的效果。大型方程的求解通常都需要使用超级计算机,消耗的计算资源非常大,而量子计算机运算速度能达到经典计算机运算速度的上万倍甚至上亿倍,这是超级计算机都难以达到的。因此,对于大型的线性方程系统、微分方程系统等的求解,量子算法拥有巨大的优势。再次,量子计算机在效率上相较经典计算机有极大的改善。IBM 的量子原型机只需 10 到 15 千瓦的功率,谷歌的 72 量子比特的量子处理器 Bristlecone 大约需要 14 千瓦,而我国的超级计算机天河二号功率能达到 24 兆瓦,每年电费都要上亿元。量子计算机源于对可逆计算机的研究。经典二进制计算机做的是不可逆运算,不可逆运算过程中要擦除无用信息,Landauer(1961)证明了擦除信息必须消耗能量,计算量越大,散发热量越多。可逆运算能够解决经典计算机中的能耗问题,量子计算机的主要功率需求是冷却超导元件,因此量子计算机消耗能量不多,相比经典计算机非常节能。

由于量子物理的特性,量子计算在技术上主要面临两方面的挑战:(1)量子的消相干现象。量子的相干性是量子进行并行运算的依据,量子计算机借助了量子纠缠的特性,但是在量子计算机中量子比特不是孤立的,量子比特一定会与外部环境发生作用,导致量子相干性衰减,也即消相干。在实际应用中,量子相干性很难保持,即使是环境中最微小的变化,例如振动或热量,也会使量子脱离“叠加态”,导致信息丢失并变得容易出错。(2)量子的不可克隆性。量子叠加态只能存在于没有被测量之前,但是当对量子系统进行测量时,输出的结果不是确定性的,量子系统会坍缩于$|0\rangle$或者$|1\rangle$态中的一个,测量的结果随机而无法控制(付震宇等,2021)。因此,任何未知的量子态不存在复制的过程,要保证量子态不变,就无法对量子进行测量,也就无法实现复制。

(四)量子计算的成本与收益

量子计算目前还处于发展的初期阶段,在生物制药、金融、军工、航空航天、交通、材料、化学、通信、气象预测、人工智能等领域都有着广阔的发展空间。但从成本收益的角度,量子计算技术的研发成本高、不确定性大,导致其未来技术应用的经济效益还存在很大的不确定性。

一方面,量子计算应用面临高昂的成本。一是极难跨越的制冷技术。量子计算机要正常工作,必须保证量子芯片始终处于接近绝对零度的极低温环境下。稀释制冷机是目前唯一能够提供长期稳定极低温工作环境的专用设备。一台稀释制冷机价格至少两三百万元,而九章量子计算原型机便

配备了 7 台。与此同时，要将计算结果传输到室温环境还需要配备特殊的数据线，一根单价在 1 万元左右，而一台计算机配备 100 根数据线就意味着 100 万元的支出。二是能耗成本。在室温下计算能耗放在豪 K(极低温)环境下则要大幅增加 100 万倍至 1 亿倍间，高达 10 兆瓦，而一般发电站的发电功率也仅在百兆瓦级别。此外，从极低温环境到室温，数据线会产生“漏热”，线路漏热能耗甚至高于计算能耗。

另一方面，量子计算能够实现巨大的经济效益。据 BCG 预测，在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，随着应用场景的增多，市场将飙升至 2600 亿美元以上。其一，当前量子计算尚无专利壁垒，抢占技术入口将获得至关重要的议价权。在经典计算机体系内，计算芯片设计与制造的核心技术掌握在科技巨头公司手中，并处于垄断地位，而在量子计算领域尚未形成垄断性巨头公司或者较高的技术专利壁垒。其二，量子计算在产业应用上大有可为。量子计算产业链以互联网头部企业及量子计算初创企业为核心，上游对传统的硅晶圆、半导体加工设备、集成电路供应商仍有一定的依赖，下游方面，化学、制药、金融等有可能从早期使用量子计算机中获益。据研究预测，2027 年全球量子计算市场将增长到 86 亿美元(刘轶男等，2022)。其三，量子计算应用领域广泛。在制药或化工领域，量子计算有望通过计算机数字形式直接帮助研究人员获得大型分子性状，加快制药行业药品研发和新型材料开发；在气象领域，量子计算可以有效和快速处理包含多个变量的大量数据，而并行计算和不断优化算法有助于提高天气预报的准确性；在军事领域，量子计算有望服务于智能决策和精准保障环节；在汽车领域，可利用量子计算技术研发性能更好的电池。此外，量子的诸多概念也可应用到行为经济学和制度经济学领域，解释经济人假设难以解释的诸多问题。如量子计算的理论也可以用来描述金融市场，量子计算适合复杂金融建模，在投资组合及衍生品定价等方面有潜在优势。

二、量子计算在经济与金融领域中的主要应用方向

现代经济与金融的发展需要使用大量的计算资源，计算机被广泛用于经济指标的历史数据分析与预测、高频交易、金融衍生品定价、投资组合优化和风险管理等领域。一方面，经济体内部高度复杂，不同参与者之间、各类资产之间具有非常复杂的网络关系，而参与者之间的互动又增加了网络的复杂性。这种复杂性使得人们难以对经济体建立有效的预测模型，极大增加了对经济指标预测的难度。另一方面，对涉及多种资产的资产价格时间序列的长期分析一直以来都是难点，这促使量子计算应用于金融问题，金融业也是最早受益于量子计算的行业部门(Herman et al，2022)。早期就有学者研究过量子物理在金融学中的应用，一些金融问题可以直接应用量子力学的形式表示(Haven，2002；Baaquie，2004)。近年来，随着中等规模量子计算机的出现，量子计算在经济金融领域的应用变得越来越可行。计算速度的微小改进，可以对金融资产回报产生巨大收益，从而激发金融机构和学者对量子计算和经济金融交叉领域的进一步研究。

(一)量子计算与经济预测

精确的宏观经济预测有助于及时评估未来的经济状况，可用于货币、财政等宏观经济政策的制定，成为经济分析的重要目标。尽管有关宏观经济预测的模型已有大量的研究，但现有模型的准确性仍然较低。GDP 增长率、CPI 就是其中两个重要的经济指标。Alminos et al(2022a)对比了量子计算技术(支持向量回归混沌量子蝙蝠算法、量子玻尔兹曼机、量子神经网络等)与深度学习方法(深度递归卷积神经网络、深度信念网络、深度神经决策树等)，发现这些模型在所有 70 个国家(47 个新兴国家和 23 个发达国家)的 GDP 增长率预测中都有非常好的表现，准确率达到 93%以上。在通货膨胀指标预测方面，Alaminos et al(2022)发现量子神经网络能够克服既有文献中预测模型预测能力不足的问题，并在通胀趋势变化的预测上能产生更低的错误率。

对于股票价格等资产价格的预测是金融机构最为关注的目标之一，并有助于辅助政府实施及时有效的政策以实现金融稳定。量子算法能够优化计算的复杂度，并提升模型预测的准确性。隐马尔可夫模型广泛应用于金融行业，但随着金融行业数据集的不断增加，传统的隐马尔可夫模型需要越

来越多的参数和时空资源来进行预测。Lu et al(2022)首次提出了一种新的基于量子隐马尔可夫算法的股票预测模型。他们发现,与金融行业用于预测股票数据的隐马尔可夫模型相比,将隐马尔可夫模型的量子版本引入到股票预测模型,可将马尔可夫模型中的概率矩阵转化为参数较少的 Karus 算子,减少参数的使用,并达到与传统隐马尔可夫模型相似的效果。Amjad et al(2018)结合了量子进化算法与模糊逻辑,提出了一种模糊时间序列(FTS)预测的新算法,用于台湾期货交易所指数以及比特币加密资产价格的预测,并发现新方法产生的预测准确性优于传统的预测模型。

复杂金融网络中金融崩溃的预测是一个计算上棘手的 NP(non-deterministic polynomial)难题,这意味着没有已知算法可以保证有效地找到最优解。金融崩溃很难预测,即使对于拥有有关金融系统的完整信息的监管机构也是如此。Ding et al(2019)通过使用 D-Wave 量子计算机实验探索解决此问题的新方法。具体而言,他们将非线性金融模型的平衡条件嵌入到高阶无约束二元优化(HUBO)问题中,而后将其转换为最多具有两个量子位相互作用的自旋 1/2 汉密尔顿量。该问题等价于找到相互作用的自旋汉密尔顿量的基态,这可以用绝热量子计算(如量子退火炉)来近似,进而计算网络受到突然冲击后机构的均衡市场价值(Orús et al, 2019a)。因此,该研究提供了一种可能更有效的方法来评估金融平衡和预测金融崩溃。此外,Alminos et al(2022b)将量子算法应用于股市下跌问题,开发了一种通过实时衰退概率预测股市崩盘的新模型。他们以 104 个国家的股市样本,发现新模型对未来全球股市低迷情景的预测具有非常好的效果。

(二)量子计算与期权定价

期权定价是金融领域中最复杂的问题之一,期权不仅仅是投资者套利的工具,更是各种对冲策略的核心。优化期权定价方法可显著影响财务运作,对金融机构的运行至关重要。

Black-Scholes-Merton(BSM)模型是一种常见的期权定价模型,它是一个简单解析可解的模型(Scholes & Blank, 1973;Merton, 1973),只需输入几个参数就可以为各种金融衍生品定价。将 Black-Scholes-Merton 公式映射到 Schrödinger 方程中即可建立量子物理与 BSM 模型的关系。Haven(2002)将期权价格设为一个状态函数,使期权价格满足 Schrödinger 微分方程,建立了一个势函数。Haven(2002)的结果验证了 Black-Scholes 模型可以在量子物理环境中实现,这为在一个没有套利的模型中以一种自然的方式包含套利提供了基础。

由于经由简化假设的模型得到的价格适用性不高,所以通常采用数值方法来进行期权定价。凭借灵活性和处理随机参数的能力,蒙特卡洛方法是最受欢迎的期权定价方法之一(Glasserman, 2003)。最早的蒙特卡洛方法应用程序是 Ulam、von Neumann、Teller 以及 Metropolis 等人在 ENIAC 上使用的(Eckhardt, 1987)。蒙特卡洛方法需要大量的计算来得到较为准确的期权价格,随着计算机的飞速发展,蒙特卡洛方法的应用也有了较大的改进。量子计算的出现大幅改善了蒙特卡洛方法的性能。

量子计算可以对蒙特卡洛方法进行加速。传统蒙特卡洛定价的金融衍生品收益的方式如下。假设风险中性概率分布可以从校准市场变量中得到或已知,用风险中性概率下的样本计算资产价格,继而计算出在这个资产价格下的期权收益。对多个样本的收益进行平均,就可以得到期权价格的近似值。假设一个单一基准资产期权的真实价格为 Π,Π 为 k 个样本的近似值,收益 $f(S_T)$ 的随机变量方差有界,即 $D(f(S_T))\leqslant\lambda^2$。通过切比雪夫不等式确定价格估算值偏离真实价格的概率为 $P[|\hat{\Pi}-\Pi|\geqslant\varepsilon]\leqslant\frac{\lambda^2}{k\varepsilon^2}$。对于恒定的概率,需要有 $k=O\left(\frac{\lambda^2}{\varepsilon^2}\right)$ 个样本来估计加性误差 ε。量子算法能够将 ε 的依赖性从 ε^2 提高到 ε,从而对误差实现二次加速。

振幅估计算法是一种实现二次量子加速的方法,Rebentrost et al(2018)设计了一个与金融导数具有相同概率分布的量子算符,并应用 Montanaro(2015)提出的量子蒙特卡洛加速方法估计其期望值,为量子计算在金融中的进一步研究奠定了基础。Rebentrost et al(2018)还进一步将这个算法应用到欧洲看涨期权定价和亚洲期权定价中发现,量子相位估计的标度指数几乎是经典相位估计的两倍。Stamatopoulos et al(2019)进一步拓展了上述期权定价方法,提出了一种基于门的在量子计算

机上实现的定价期权和期权投资组合的算法。该算法在保留量子振幅估计加速的基础上使用了少量的门来衡量期权价格,给出了能够显著减少由噪声二量子位门引起的误差的方法。然而,他们同时也指出,目前可用的量子处理器还不能够为金融行业的典型投资组合定价,需要使用包含更深的量子电路的量子硬件。

不仅是蒙特卡洛方法,对于其他衍生品定价模型,例如利率定价,多因素 Heath-Jarrow-Morton 模型最为适合。对远期利率建模时需要考虑噪声成分,以捕捉远期利率的动态。然而,由于没有通用的解析解可用,通常需要在考虑的噪声因素数量和执行数值模拟的计算时间之间进行权衡。Martin et al(2019)提出了一种量子主成分分析方法来减少噪声因子的数量,并用 5 量子比特的 IBM QX2 量子计算机对由 2 个和 3 个远期利率的历史数据构成的 2×2 和 3×3 互相关矩阵的主成分进行了实验估计,结果表明量子计算机在金融领域的实际应用完全可以实现。此外,Adam(2022)提出了量子电路模型,描述了与保险相关的赔付特征,将其应用于保险合同的定价问题上。

除了定价模型,隐含波动率也是一个对期权定价至关重要的指标。Sakuma(2020)在 Beer et al(2020)提出的深度量子神经网络基础上,提出了一种用于学习隐含波动率的量子方法。近年来对通过量子计算来加快神经网络和深度学习算法的研究层出不穷。在现有的量子退火机上训练神经网络会极大地节约计算资源,而且更不易陷入局部极小值,一旦训练完成,这个神经网络算法就可以在任何经典计算机上运行。Benedetti et al(2016)已经证明了玻尔兹曼机可以在 D-Wave 量子处理器上进行有效的训练。目前,也有学者尝试设计量子神经网络算法,如量子感知器算法(Roget et al,2021)、量化投资中常用的量子隐马尔可夫模型(Monras, 2010)等。量子神经网络算法目前还处于起步阶段,未来还需进一步研究发展。

Baaquie 将量子力学和量子场论充分运用于衍生品定价问题的研究中。传统的金融数学以随机微积分为基础,Baaquie(2007)强调了路径积分和汉密尔顿(Hamilton)量的重要性,也即将 Feynman-Kac 方程作为金融衍生品定价理论的基础。Baaquie(1997)利用路径积分重新构建了 Merton-Garman 方程,使得股票期权定价结果更为准确。他还针对简单的期权定价模型(如 Black-Scholes 模型)给出了一些用于期权定价的路径积分的晶格模拟方法,概述了该方法在非线性系统中的应用;利用路径积分将 Heath-Jarrow-Morton 模型推广到允许所有远期利率独立波动的情况,由此产生的理论被证明是二维高斯量子场论。Baaquie(2004)认为金融衍生品的定价也可以使用基于汉密尔顿公式的量子力学工具进行建模和模拟,并通过郎之万和蒙特卡洛方法模拟了这些方法在期权定价中的应用。

(三)量子计算与投资组合

投资组合问题可以表述为等式约束的二次规划问题:在固定的风险下找到预期收益最大化的投资组合,或者在固定的预期收益下找到风险最小化的投资组合。确定最佳投资组合需要进行大量的计算,对于经典计算机来说消耗的计算资源和时间较多,量子计算机是确定最佳投资组合极好的工具。

量子算法用于确定最佳投资组合所花费的时间远小于经典算法,在实际交易中非常有益。Michael(2010)从基本的随机方程出发,得到了一个依赖于可观测测量值的风险中性估值模型,进而推导出连续变量下的量子算法资产组合模型,建立了金融风险分析和量子计算的联系。Rebentros & Lloyd(2018)用量子线性系统算法得到风险—收益曲线并确定给定回报下的最小风险投资组合,最终该投资组合以量子态的形式呈现。该算法理论上可以达到 poly(log(N))的运行时间,其中 N 是历史收益数据集的大小,而用于确定最佳投资组合的风险—收益曲线和其他属性的经典算法需要花费的时间为 poly(N)。风险的测定是投资组合问题的关键,Woerner & Egger(2018)构造了一种量子算法来模拟说明量子计算机如何确定由不同到期日的政府债务组成的两种资产组合的金融风险,结果显示,与蒙特卡洛方法相比,收敛速度是二次加速的。Kerenidis et al(2019)首次提出了求解有约束投资组合优化问题的量子算法,该算法基于二阶锥规划的量子内点法,允许对设计变量施加非负性和预算约束,与目前最好的经典算法相比能够实现一个多项式的加速。

一些学者也在尝试将量子计算用于模拟二级市场。Schaden(2002)用投资者持有证券和现金的所有可能结果作为基底来构造市场状态的希尔伯特空间,还构造了表示现金转移和证券买卖等基本

金融交易的线性算子,给出了产生现金流和证券交易的时间演化的简单汉密尔顿模型。他用持有数的增减来定义生成算子和湮灭算子,由此用量子理论的方法导出了市场演化的 Schrödinger 方程。同时,他还将市场的运行归因于市场参与者对资产的持有数,通过持有数的变化来描述市场的行为。Cohen et al(2020)研究了如何利用量子计算机从 60 只美国上市、流动性强的股票中构建最佳投资组合,利用 D-Wave2000Q 量子退火机寻找最优风险与收益的组合。结果表明,D-Wave2000Q 量子退火机可以利用少量样本产生一组理想的投资组合。Racorean(2015)研究发现,在量子计算中,为了解决一个特定的问题,一系列的量子门必须按照预先确定的顺序排列,形成一个量子电路。如果量子门的序列是已知的,所要解决的问题和所定义的量子电路的结果是未知的,那么正好可以表示股票市场的情况。他使用股票投资组合的价格时间序列模拟了任意子假设量子计算模型中的量子门。根据伊辛任意子模型为四只股票组成的投资组合构造了 1 量子比特的量子门,加入两只股票就会产生 2 量子比特的量子门,再加上其他股票时,就会形成一系列 n 量子比特的量子门,形成一个量子码。量子门在股票投资组合的变化中连在一起,形成量子电路。股票市场的千变万化导致表示股票市场的量子电路不同于其他固定的量子电路,它是任意的。

最佳投资组合的确定是一个优化问题,而由于优化问题是个 NP(non-deterministic polynomial)难题(Emms et al, 2009),对于经典计算机来说,实现最优化的选择是非常困难的,但量子优化算法可以解决这个问题。量子优化算法的核心是绝热量子计算(Farhi et al,2000),量子退火是实现绝热量子计算的物理过程。但是量子退火过程很难满足绝热量子计算所需的条件,因此量子退火是绝热计算的一种近似实现。Zagoskin(1986)证明了近似绝热计算可以找到接近最优的解。Rosenberg et al(2016)在 D-Wave 的量子退火机上求解了这个问题,结果显示成功率很高。未来当量子退火机能处理更大的问题时,量子退火将完全取代传统的方法。量子退火机还可以解决最优套利问题,量子退火机产生的最优解与经典解相同,所用时间更短。最优套利问题是一个二次无约束二值优化问题,Rosenberg(2016)给出了求解最优套利机会的两个公式,提出了基于交易者对风险的厌恶程度,找到利润和风险最平衡的套利机会。Venturelli & Kondratyev(2018)研究了均值—方差投资组合优化问题的混合量子经典解法。他们遵循现代投资组合理论的原则,从真实的金融统计数据出发,生成了投资组合优化问题的参数化样本,并在 D-Wave2000Q 量子退火机上进行了模拟。Egger et al(2020)从凸优化、组合优化、混合二进制优化问题等方面总结了相关量子优化算法,并给出了在投资管理、投资组合优化、拍卖等领域的应用实例。目前关于量子优化在金融领域应用的研究还不多,多数还停留在原理的证明上。但是量子计算在优化问题上已经有了较多的研究,优化问题在金融领域的应用也有很多。相信未来会有更多的学者关注量子优化与金融的交叉领域,量子计算将在金融优化问题上展现它的实用价值。

除了量子算法以外,还有学者将量子力学与金融学结合起来研究。比如,Ilinski(2001)用量子场论描述金融市场,将金融市场看作由投资组合构成的"金融场",一个坐标代表组合的价值,其余的坐标代表在组合中各种资产所占的比例,金融行为相当于场中的运动。他运用场论方法推导了资产价格和资金流量随时间演变的过程。Da Cunha & Silva(2019)研究了 17 种与量子系统类似的数字货币,在金融资产和量子系统之间建立联系。他们提出了"特征组合"的概念,发现数字资产具有较高的可解释方差,市场倾向于价值显著不同的资产。

量子计算能大大提高金融机构在高频交易、对冲、衍生品定价、套利等方面的能力。面对海量的信息,金融交易往往比拼的是计算的速度和精度,量子计算的高效计算能力有助于模型的改进,能够使得到结果的时间更短、模型结果更加精确,提高资产交易效率,进而从中获益。

(四)量子计算与银行业务

为防范金融风险,《巴塞尔协议》采用资本充足率这个指标来约束银行。资本充足率不仅能控制银行规模,而且也能反映银行风险,是当前银行监管的一个重要指标。资本充足率也即资本/风险加权资产,风险加权资产是根据风险的大小对资产进行加权计算得到的。这表明,监管部门对银行的资本金要求与风险模型的准确性密切相关。因此,风险模型的准确性对于银行来说意义重大。量子

计算不仅能够提高精度，还能提高速度。风险价值（VaR）函数是常用的量化风险的工具，它衡量了投资组合损失的分布。另一个更好的风险评估工具条件风险值（CVaR）衡量的是在投资组合的损失超过某个给定 VaR 值时的平均损失值。VaR 和 CVaR 的估计通常用到蒙特卡洛抽样的相关概率分布，Woerner & Egger（2018）率先提出了采用量子计算加速蒙特卡洛来改进这些估计的方法，并在 IBM Q 上进行了测试，结果显示，量子计算能够以极高的精度确定 VaR 和 CVaR，相较于经典方法有二次加速。

智能化是银行业的一个发展趋势。基于机器学习的人工智能在信用评分、反洗钱、预测分析、风险管理以及智能营销等领域都有重要的应用，这些领域的智能化是大势所趋。量子计算能显著有效地加速大规模神经网络中的深度学习，提高其数据处理速度和处理量，从而进一步提高银行业的智能化水平。机器学习是一种综合了计算机科学、统计学、工程学、生物学等多学科的交叉学科，是人工智能的重要组成部分（Taddy，2018），被广泛应用于金融等多个领域。机器学习需要进行大量的矩阵运算，自 HHL 算法出现以来，量子机器学习得到极大的发展。量子机器学习可分为两类：一是寻找量子版本的机器学习算法，二是应用经典机器学习优化量子系统。量子计算能够降低计算复杂度，改善泛化性能，使得传统的机器学习算法在效率上有了极大的改进；传统机器学习算法的量子版本包括最小二乘拟合、支持向量机、主成分分析和深度学习等。传统机器学习算法也能用来改善量子计算系统的基准和控制（Orús et al，2019b）。在大数据时代，多数银行都已经开始通过大数据技术来开展业务，比如为客户画像、精准营销、运营优化等。大数据的使用依赖庞大的数据库，这对银行来说是个不小的资源负担。量子比特的叠加特性决定了量子服务器的存储能力远超现有经典服务器。通过优化传统的机器学习算法，量子计算还能大幅提高数据处理能力，节约服务器资源。尤其是当量子计算机投入使用后，服务器的散热问题也能得到有效解决。在智能营销、智能风控等对计算速度和精度要求较高的领域，量子计算支持开发更智能、更灵敏的计算机学习系统，在算法能力和速度方面具有显著优势，能够彻底解决银行的“计算能力瓶颈”问题。例如，量子算法可显著提升支付系统的流动性效率。McMahon et al（2022）在混合量子退火求解器上开发了一个优化支付效率的算法，研究发现，加拿大高价值支付系统（HVPS）若采用该算法，则平均每天可节省 2.4 亿加元的流动性。

对于银行来说，评估与贷款相关的风险至关重要。在发放贷款前，银行会考虑贷款人的收入、年龄、财务历史等方面情况，识别他们是高风险或低风险客户，进而考虑是否发放贷款，这称为申请评分。申请评分与行为评分、催收评分共同构成了信用风险 ABC 模型。评估信用风险问题非常适合应用机器学习和优化问题求解，量子计算的引入能够大幅改善评估信用风险的精度，减少所需时间。分类算法（Baesens et al，2003）是其中的关键（Lessmann et al，2015）。将每个客户属性表示为一个向量，这样所有的客户就构成了一个向量空间。标记训练集能将每个向量都归属一个类别，也即每个客户都有对应的贷款风险。当给定一个新的向量时，程序能够将其划分至最有可能的分类中。根据训练集的大小和考虑的属性数量，找到一个新的向量类需要执行大量的高维投影操作，这将会降低可信度。量子计算机的出现解决了这个问题，它能更有效地完成投影操作。Aïmeur et al（2006）基于 Buhrman et al（2001）的工作，将每个向量表示为一个量子态，通过重复执行互换测试，有效地估计了量子态之间的距离。Lloyd et al（2013）提出了一种将经典数据编码成量子态的替代方法，效率优于经典算法。信用评分时客户有些数据参考价值不大，Milne et al（2017）在信用评分时去掉了这些相关度小的特征，利用剩下的数据，将其转化为量子退火机上运行的二次无约束二值优化问题。他们使用了加州大学欧文分校的德国信贷数据进行实验，结果表明，与许多软件中使用的递归特征消除（RFE）技术相比，在没有损失精度的情况下，二次无约束二值优化问题特征选择产生了更小的特征子集。这也意味着量子退火机能够以编程方式降低特征集维数，未来的量子退火机也可以用于确定信用分析的最优特征。

（五）量子计算与数字货币

量子计算的出现还催生了量子货币的概念。量子货币实质上就是基于量子密码学的数字货币。利用不可克隆定理、不确定性定理和量子的叠加态能够实现加密，使得量子货币在物理上无法伪造。

这一方法最早由 Stephen Wiesner 于 1970 年左右提出(Wiesner, 1983)。每张钞票由一个经典序列号 S 和包含 n 个无纠缠量子比特的量子态构成。银行将维护一个包含了这些量子态的巨大的数据库,当客户想验证钞票时,银行将对量子态中每个量子比特进行验证。Molina et al(2012)证明了他人复制钞票成功的概率为$(3/4)^n$。

在 Wiesner 建立的量子货币方案中,只有印发钞票的银行才能验证钞票,每一个流通中的钞票都需要在数据库中有一个入口。Bennett et al(1983)的工作减小了数据库的大小:通过一个伪随机函数 f_k 生成一个新的量子态,其中密钥 k 只有银行知道。但是该方法并不绝对安全,在给定指数时间下,伪造者能够通过 Shor 算法计算得到 k。关于量子货币的早期探索也激发了学者对量子密码学的研究兴趣(Bennett & Brassard, 2020)。Lutomirski(2009)发现伪造者可以通过验证过的钞票来伪造钞票。Mosca & Stebila(2010)建议银行使用一种盲量子计算协议,伪造者即使能够验证量子货币,也不能制造更多的量子货币,这样可以将钞票的验证工作转交给第三方。Gavinsky(2011)在 Molina et al(2012)、Pastawski et al(2011)的工作基础上提出了 Wiesner 体系的变体,只需第三方和银行之间进行经典通信。

Aaronson(2009)提出了一种公开密钥量子货币,任何人都可以进行验证。Lutomirski(2010)证明了该方案并不安全可靠。Lutomirski(2011)提出了一种基于扭结不变量理论的公开密钥量子货币方案,该方案安全性尚未被证明。Farhi et al(2012)在此基础上加入了链接图和亚历山大多项式,每张钞票都是指数多方向链接图的叠加,实现了同样的结果。

三、量子计算影响经济与金融发展的理论机制

量子计算在经济与金融领域中的应用正在飞速发展,作为一项新兴数字技术,量子计算有望对经济与金融领域的创新发展产生重要影响。一方面,量子计算凭借高效存储能力和计算效率,能在解决限制经济与金融发展的传统因素方面发挥重要作用,例如降低信息不对称、降低金融交易的成本、提高全要素生产率与运行效率。另一方面,量子计算的快速发展可能对经济与金融的发展带来威胁和挑战。由于技术内在的"双刃剑"属性,量子计算在缓解传统信息不对称的同时,也会加大市场交易双方的技术不对称,从而引发新的道德风险,甚至是科技伦理问题。同时,量子计算对计算速度的巨大突破可能会造成用户数据、隐私的泄露,并可能通过破解安全密钥引发用户财产的损失,导致数字货币安全性面临极大的挑战。

(一)量子计算优化经济与金融运行的内在机理

1. 降低信息不对称。量子计算的应用使得金融业在降低信息不对称方面比以往传统的方法显著得多。风险越高的客户,越可能产生广泛的边际效应,从而导致更多的违约,加剧利率的上升(Livshits et al, 2016)。Baesens et al(2003)认为量子计算更完美地解决了客户分类问题,更有效地评估客户的贷款风险,从根本上克服了银行业的信息不对称。量子计算的高效存储能力也能解决传统的信贷市场中仅仅依靠客户的财务信息等进行决策的不足。客户的社会关系、网络上留下的数据记录等也是信贷关系的重要影响因素(Lin et al,2013,Berg et al,2020),特别是全球进入智能化时代,网络上的数据记录将越来越丰富,越来越能反映客户的偿债能力。将它们作为信贷审核的补充,将大幅降低信息不对称程度,使得贷款方风险更低、利润更高(Chade & Silvers, 2002)。量子计算可以有效利用客户社会关系、浏览记录等充分挖掘客户信息,利用纠缠性原理描述客户千丝万缕的社会联系并合理刻画客户特征,增加客户的借贷渠道与成功概率,降低违约风险。

此外,相较于传统的方法,机器学习的应用在对财务造假的识别上具有得天独厚的优势(Hajek & Henriques, 2017),而量子计算的引入能够应用更多信息、更精准快速地通过机器学习实现对财务造假的识别。金融投资者离不开对市场信息的把握与预测。金融市场的嘈杂性、动态性以及非参数特点使得传统的计量模型很难对庞杂的数据进行精准的建模(Längkvist et al, 2014)。回归模型是预测中的常用方法之一,一般通过最小化训练数据与模型预测值之间的最小二乘法来找到最优拟合参数,在这个过程中需要寻找训练数据矩阵的逆,计算量较大。Wiebe et al(2012)研究发现,对于

稀疏训练数据矩阵，可以将模型的最佳拟合参数转化为量子态的振幅，即便与最快的经典计算机上的算法相比，也实现了指数级的加速。Wang(2017)在此基础上将该算法推广到非稀疏训练数据矩阵。当使用大量高维复杂数据进行分析预测时，就显示了主成分分析法这种降维分析方法的优势(Orús et al，2019b)。主成分分析法需要寻找一个高维矩阵的主导特征值和特征向量。一个N×N矩阵的时间复杂度为$O(N^2)$，当N特别大时，其计算成本非常高。Lloyd et al(2014)提出了一种量子主成分分析算法，能够在量子计算机上以指数级速度运行。这极大地拓宽了主成分分析法的应用范围，使得金融机构能够从文本、图像、音频等中提取大量信息，充分利用这些信息进行预测，降低信息不对称。

2.降低金融交易成本。降低交易成本是金融业增加利润的重要途径之一，量子计算的运用能从以下几方面降低金融交易成本。(1)信息搜寻成本。对于需要信息的信贷市场来说，可以利用量子计算充分搜集、提取、整合有用信息，大量透明的信息可以降低贷款方的审核成本，减少违约风险(Sutherland，2018)。作为一种前沿数字技术，量子计算也能降低交易双方匹配的搜寻成本(Thakor，2020)。在风险识别、精准营销、智能投顾咨询等方面，量子计算等数字技术的出现使得金融机构进一步规避了风险，降低了获得客户的成本(Gomber et al，2018)，也减少了服务单一客户的成本，从而减少了客户获得金融服务的成本(Philippon，2019)。(2)信息处理成本。在信贷市场中，要想准确地判断客户是否可以进行借贷，银行会希望在信用评分时尽可能多地考虑不同的因素。然而验证大量因素的准确性成本较高(Milne et al，2017)，因此贷方可能愿意牺牲评价的准确性来降低验证贷款申请准确性的成本。量子计算的出现可以利用组合学来生成准确的决策而无须花费太多的成本。量子计算还可以用于机器学习算法中，建立信用评估模型，降低风险评估成本(Livshits et al，2016)。(3)信息存储成本。量子存储最初用于远程通信中，量子比特的叠加特性决定了量子服务器的存储能力远超现有的经典存储服务器。量子计算还能优化传统机器学习算法，大幅提高数据处理能力，节约服务器资源(Orús et al，2019b)。尤其是当量子计算机投入使用后，服务器的散热问题也能得到有效解决，使得信息存储成本大幅下降，因此可以用于金融机构建造大型基础数据平台，夯实数据基础。

3.提高经济全要素生产率与运行效率。量子计算作为重要的技术革新，推动了技术进步，进而可以推动经济全要素生产率的提高。各个行业都能享受到技术溢出带来的全要素生产率的增长(Han et al，2011)，例如在银行业中，不仅是进行技术改革的银行，所有的银行都能享受到全要素生产率提升带来的益处，规模越小的银行得到的益处越多(Lang & Welzel，1996)。新技术的运用还能增加金融机构的创新能力，研究表明，规模越小的机构创新能力越强(Vives，2019)。技术进步还能改变金融结构(Thiel，2001)，推动金融产业升级，提升运行效率。量子计算的出现为产品和服务的销售提供了新的可能，在未来还可能引起支付方式的再一次革命性改变(Chen et al，2017)，此外还能提高风险管理效率(Gomber et al，2018)。量子计算在经济预测、期权定价、投资组合等中的应用还能减少政策制定者、投资者的行为偏差，提高决策效率(D'Acunto et al，2019)。

(二)量子计算威胁经济与金融发展的潜在机制

1.产生新的道德风险。量子计算也可能造成客户与金融机构双方在知识、技术方面的地位落差，使得没有掌握技术的一方处于不利位置。多数客户只能得知决策结果，难以了解决策过程，对其中是否涉及伦理冲突等无法得知。金融机构可以利用这种技术进步，有效地使用获得的信息，以便对不同客户实施不同的策略从而获得更高的利润。这种差别定价难以被客户识别，金融机构能够尽可能多地获得消费者剩余，甚至可以通过继续细分客户类型，实行阻止价格竞争的激进定价策略来固定客户(Grover & Ramanlal，1999)。但是当客户私下对金融机构的决策过程信息知情时，客户的决策行动往往会发生扭曲(Chade & Silvers，2002)，当金融机构通过跟踪得知客户了解自身决策行为后，也会减少从知情的客户处获得的利润，客户与金融机构之间的互动也变得越来越复杂(Deck & Wilson，2006)。随着技术的发展，量子计算改变社会的作用增强，也许会远离人类的最初目标和控制。因此要对新技术带来的一切变化保持觉察，及早认识到科技给社会带来的诸多问题，寻求最

大范围内的共识与解决方案,鼓励“技术向善”,实现经济社会的良性发展。

2.引发科技伦理问题。量子计算可能造成现有数据、隐私的泄露以及资产的不安全。数据安全性和机密性至关重要,现有的密码系统通过使用加密和签名算法进行安全通信来提高数据安全性和机密性。金融部门的数据和通信安全依赖于公共密钥,公共密钥能够支撑包括认证/授权、隐私/机密、完整性在内的安全服务(Burr & Lyons-Burke, 1999)。量子计算机的出现使得公共密钥不再安全可靠。对于网上银行交易的认证、ATM 存取款等业务,攻击者可以用量子计算机破解公共密钥来伪造交易。

广泛应用于银行、互联网等领域的公开密钥体系 RSA 依赖于大数因子分解,通过使用两个大素数的乘积来生成公钥和私钥。Shor 算法是用于大数因子分解的量子算法,自其发表以来,RSA 的安全性就受到了质疑。传统的算法进行大数因子分解时间复杂度为 log(N),分解一个 1000 位的数需要 10^{25} 年,而量子计算机采用 Shor 算法只需不到一秒就能分解完成。传统的算法破解 RSA 复杂度高、流程复杂、成本过高,目前银行业多采用增加密钥长度的方式来提高安全性。但是量子算法高效的并行计算能力使得这些加密措施都不再有效,只要量子计算机进入商用阶段,RSA 体系就将透明化,银行的信息安全将面临巨大挑战。

除了 RSA 以外,DES 也是一种常见的加密算法。DES 是一种对称密码体制加密算法,常用于 POS 机、ATM 机、IC 卡等场景。密钥长 64 位,其中 56 位参与运算。破解 DES 算法的唯一方法就是穷举法,5 位密钥穷举空间为 256。然而现行的二进制计算机破解 DES 算法搜索 256 个穷举空间需要上千年。Grover 搜索算法可以用来破解 DES 体系,Grover 算法利用量子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,能以“指数减半”的方式大幅提高搜索效率,4 分钟内就能破解 DES 算法(Long, 2001)。

随着量子计算的不断发展成熟,未来会有更多的针对银行加密体系的量子算法被开发出来。因此,对于信息加密来说,量子计算的影响是两方面的。它既能凭借高速并行计算能力和量子的叠加性、纠缠性等特性提高信息加密水平,也会对现有的加密体系造成严重的冲击。一旦有国家成功研制能够破解现有加密系统的量子计算机,其他国家的信息安全将得不到保障。据美国中央情报局(CIA)前雇员斯诺登透露,美国国家安全局(NSA)早在 2014 年就已经开始秘密研制能够破解加密系统的量子计算机(Rich & Barton,2014)。因此,我国必须重视量子计算带来的威胁,加快加密系统的升级迫在眉睫。

目前,中国和美国、日本以及欧洲等国家都在积极地推动抗量子计算攻击的密码体系研究。量子计算对非对称密码体系威胁较大,对对称密码等密码体系威胁较小,通过 Shor 算法几个小时内就可破解非对称密码体系(Gidney & Ekerå, 2021)。因此,可以通过升级传统的密码体系来对抗量子计算的威胁。抗量子计算攻击的传统密码体系包括基于编码的加密体系、基于多变量的加密体系、基于格的加密体系和基于哈希的签名体系四种(Craig, 2009)。但是,这些体系都没有经过严格的证明,其有效性还需量子计算发展的实践检验。因此准确来说,抗量子计算攻击的密码体制还没有真正建立起来。通过物理手段构建新的信息安全保护架构也能对抗量子计算对密码学的冲击。区块链就是一种新的安全保护架构。量子加密技术使得区块链中节点之间能够安全验证对方身份,防止信息被恶意篡改。俄罗斯开发了全球首个量子区块链系统,并在 Gazprom 银行进行了验证,结果表明,该量子区块链系统能够有效防止区块链被量子计算攻破,保证密码体系的安全(Kiktenko et al, 2018)。但目前也有学者指出一台 4000 量子比特的量子计算机就能瓦解区块链,因此对抗量子计算的攻击也不能只依靠区块链技术,还需研究更多的方法。

3.伪造数字货币。经典比特能够进行无限复制,这也是数字经济的基础。但对货币来说可复制并不是一个好的特性,当前包括比特币在内的数字货币在现有的计算能力下具有极高的安全性,但是若量子计算机发展到实用阶段,则数字货币的安全性将面临严峻挑战。对数字货币来说,用户唯一的保护是他们的数字签名,而银行客户则受到银行卡、安全问题、身份检查和人工柜员的保护。拥有量子计算机的不法分子可以使用 Shor 量子算法破坏基于密码算法的安全协议,伪造任何数字签

名，冒充该用户并盗用他们的数字资产（Fedorov et al，2018）。数字签名的破解是非常紧迫的威胁。有研究认为，破解数字签名需要一台通用量子计算机，然而也有学者认为使用 D-Wave、谷歌等公司的一些功能更有限的新型量子设备也能破解数字签名，而这在未来很短的时间内能够实现（Peng et al，2008）。

四、总结

量子计算的出现是人类发展史上的一个里程碑，将带来新一轮的科技革命。经济与金融领域诸多问题都需要精密的计算，消耗大量的计算资源，而量子计算在此方面优势明显。随着量子计算技术研发的不断突破，高成本瓶颈逐渐克服，量子计算未来不仅能在经济与金融领域深入应用并且取得可期的经济效益，也将给化工、医疗、通信、军事、气象、汽车、人工智能等领域带来颠覆性改变。本文对量子计算在经济与金融领域应用的研究文献进行了较为系统的梳理和总结，分析了量子计算促进经济与金融发展的方向，量子计算影响经济与金融发展的理论机制以及未来量子计算技术发展和应用存在的潜在挑战。

第一，随着量子计算机的发展，量子优化将会在经济与金融领域发挥重要的作用。量子算法的高效率可以有效地提升经济预测效果、改进期权定价与投资组合的选择，与现有的方法相比在速度和准确性方面都有很大的改善。量子计算非常适用于金融中财务相关的优化问题，但目前还停留在原理证明上。量子计算的出现也将给传统银行业带来重大影响，如量子计算的高效并行计算能力可以有效改善商业银行的信用评分与风险模型，特别是量子学习算法的出现，使得机器学习的性能有了大幅提升。量子计算的出现还催生了量子货币的概念，量子货币实质上就是基于量子密码学的数字货币。

第二，量子计算影响经济与金融发展有其内在机理。一方面，在优化经济与金融运行方面，量子计算凭借高效存储能力和计算效率，能够降低信息不对称、降低金融交易的成本、提高经济全要素生产率与运行效率，从而改善传统因素对经济与金融发展的制约。另一方面，由于技术内在的“双刃剑”属性，量子计算促进经济与金融发展的同时也带来了挑战。量子计算在缓解传统信息不对称的同时，也会加大市场交易双方的技术不对称，从而引发新的道德风险甚至是科技伦理问题。同时，量子计算对计算速度的巨大突破可能会造成用户数据、隐私的泄露，并可能通过破解安全密钥引发用户财产的损失，导致数字货币安全性面临极大的挑战。特别是在银行业，RSA 和 DES 加密体系在量子计算面前近乎透明，银行在信息加密方面亟须改进。

第三，虽然量子计算相比目前的经典算法和计算机有着巨大的优势，但是现有量子计算机还处于初级阶段，在技术方面和非技术方面都面临一些困难，能够进入实际应用阶段的时间还不明确。在技术挑战方面，量子计算目前还处于原型机研发阶段，对环境的微小变化非常敏感，也更容易出错，且拓展性问题面临挑战。在非技术挑战方面，关于量子计算的研究至少包括量子算法、量子程序设计、量子计算机体系结构、量子计算物理实现等多个层次。这些研究分布在不同学科领域，需要物理学、计算机科学等多个学科的交叉合作，而跨学科的交叉融合研究尚有较大发展空间。

第四，主要国家在量子计算领域竞争激烈，美国、英国、日本、韩国等国家都高度重视并将量子技术作为引领未来的颠覆性、战略性技术，美国还将量子技术纳为限制性出口技术，但关于实用化量子计算机的竞赛仍处于起跑阶段。我国量子计算领域的发展具有紧迫性，要发挥我国长期积累的、在物理和材料等学科的研究基础优势，构建量子计算研发生态系统，加快量子计算技术攻坚，在量子计算工程化应用和产业化发展领域下好先手棋，抢占量子科技国际竞争制高点。

参考文献：

付震宇 等，2021：《量子计算技术发展路线与趋势分析》，《中国电子科学研究院学报》第 8 期。

刘晓楠 等，2021：《Grover 算法改进与应用综述》，《计算机科学》第 10 期。

刘轶男 杨巍 魏凡，2022：《量子计算发展与应用动向研究》，《中国电子科学研究院学报》第 2 期。

龙桂鲁 等，2004：《Grover 量子搜索算法及改进》，《原子核物理评论》第 2 期。

Aaronson，S.（2009），“Quantum copy-protection and quantum money”，The 24th Annual IEEE Conference on Computational Complexity，15th－18th July，Paris，France.

Adam, M(2022), "Potential applications of quantum computing for the insurance industry", arXiv preprint arXiv: 2210.06172.

Aharonov, D. & M. Ben-Or(1997), "Fault-tolerant quantum computation with constant error", *Proceedings of the Twenty-Ninth Annual ACM Symposium on Theory of Computing*, 4th－6th May, Texas, United States.

Aïmeur, E. et al(2006), *Machine Learning in a Quantum World*, Springer.

Alaminos, D. et al(2022), "Quantum neural networks for forecasting inflation dynamics", *Journal of Scientific & Industrial Research* 79(2):103－106.

Alaminos, D. et al(2022a), "Quantum computing and deep learning methods for GDP growth forecasting", *Computational Economics* 59(2):803－829.

Alaminos, D. et al(2022b), "Forecasting stock market crashes via real-time recession probabilities: A quantum computing approach", *Fractals* 30(5):1－16.

Amjad, U. et al(2018), "A quantum based evolutionary algorithm for stock index and bitcoin price forecasting", *International Journal of Advanced Computer Science and Applications* 9(9):123－132.

Baaquie, B. E(1997), "A path integral approach to option pricing with stochastic volatility: Some exact results", *Journal de Physique I* 7(12):1733－1753.

Baaquie, B. E. (2001), "Quantum field theory of treasury bonds", *Physical Review E* 64(1): 016121.

Baaquie, B. E. et al(2004), "Hamiltonian and potentials in derivative pricing models: Exact results and lattice simulations", *Physica A: Statistical Mechanics and Its Applications* 334(3－4): 531－557.

Baaquie, B. E. (2004), *Quantum Finance*, Cambridge University Press.

Baaquie, B. E. (2007), *Quantum Finance: Path Integrals and Hamiltonians for Options and Interest Rates*, Cambridge University Press.

Baesens, B. et al(2003), "Benchmarking state-of-the-art classification algorithms for credit scoring", *Journal of the Operational Research Society* 54(6):627－635.

Beer, K. et al(2020), "Training deep quantum neural networks", *Nature Communications* 11(1):1－6.

Benedetti, M. et al(2016), "Estimation of effective temperatures in quantum annealers for sampling applications: A case study with possible applications in deep learning", *Physical Review A* 94(2):1－13.

Benioff, P. (1980), "The computer as a physical system: A microscopic quantum mechanical Hamiltonian model of computers as represented by Turing machines", *Journal of Statistical Physics* 22(5):563－591.

Bennett, C. H. & G. Brassard(2020), "Quantum cryptography: Public key distribution and coin tossing", arXiv preprint arXiv:2003.06557.

Bennett, C. H. et al(1983), "Quantum cryptography, or unforgeable subway tokens", in: D. Chaum, et al(eds), *Advances in Cryptology*, Springer.

Berg, T. et al(2020), "On the rise of FinTechs: Credit scoring using digital footprints", *Review of Financial Studies* 33(7):2845－2897.

Bharti, K. et al(2021), "Noisy intermediate-scale quantum (NISQ) algorithms", *Reviews of Modern Physics* 94: 015004.

Biamonte, J. et al(2017), "Quantum machine learning", *Nature* 549(7671):195－202.

Black, F. & M. Scholes(1973), "The pricing of options and corporate liabilities", *Journal of Political Economy* 81(3):637－654.

Buhrman, H. et al(2001), "Quantum fingerprinting", *Physical Review Letters* 87(16):167902.

Burr, W. & K. Lyons-Burke(1999), "Public key infrastructures for the financial services industry", National Institute of Standards and Technology, https://tsapps.nist.gov/publication/get_pdf.cfm? pub_id=151200.

Campbell, E. T. et al(2017), "Roads towards fault tolerant universal quantum computation", *Nature* 549(7671):172－179.

Chade, H. & R. Silvers(2002), "Informed principal, moral hazard, and the value of a more informative technology", *Economics Letters* 74(3):291－300.

Chen, Y. A. & X. S. Gao(2022), "Quantum algorithms for Boolean equation solving and quantum algebraic attack on cryptosystems", *Journal of Systems Science and Complexity* 35(1):373－412.

Chen, Y. A. et al(2018), "Quantum algorithms for optimization and polynomial systems solving over finite fields", arXiv preprint arXiv: 1802.03856v2.

Chen, Z. et al(2017), "The transition from traditional banking to mobile internet finance: An organizational innova-

tion perspective－A comparative study of Citibank and ICBC", *Financial Innovation* 3(1):1－16.

Childs, A. M. et al(2017), "Quantum algorithm for systems of linear equations with exponentially improved dependence on precision", *SIAM Journal on Computing* 46(6):1920－1950.

Cohen, J. et al(2020), "Portfolio optimization of 60 stocks using classical and quantum algorithms", arXiv preprint arXiv:2008.08669.

Cornuejols, G. & R. Tutuncu(2018), *Optimization Methods in Finance*, Cambridge University Press.

Craig, G.(2009), "Fully homomorphic encryption using ideal lattices", *Proceedings of the Forty First Annual ACM Symposium on Theory of Computing*, 31st May－2nd June, Maryland, United States.

D'Acunto, F. et al(2019), "The promises and pitfalls of robo-advising", *Review of Financial Studies* 32(5):1983－2020.

Da Cunha C. R. & D. R. Silva(2019), "On the quantum behavior and clustering properties of correlated financial portfolios", arXiv preprint arXiv:1910.08627.

Deck, C. A. & B. J. Wilson(2006), "Tracking customer search to price discriminate", *Economic Inquiry* 44(2):280－295.

Deodoro, J. et al(2021), "Quantum computing and the financial system: Spooky action at a distance?", IMF Working Papers, No. 071.

Deutsch, D.(1985), "Quantum theory, the Church-Turing principle and the universal quantum computer", *Proceedings of the Royal Society of London, A. Mathematical and Physical Sciences* 400(1818):97－117.

Deutsch, D. & R. Jozsa(1992), "Rapid solution of problems by quantum computation", *Proceedings: Mathematical and Physical Sciences* 439(1907):553－558.

Dieks, D.(1982), "Communication by EPR devices", *Physics Letters A* 92(6):271－272.

Ding, Y. et al(2019), "Towards prediction of financial crashes with a D-Wave quantum computer", arXiv preprint arXiv:1904.05808.

Douglas, B. L. & J. B. Wang(2017), "Classical approach to the graph isomorphism problem using quantum walks", *Journal of Physics A. Mathematical & Theoretical* 41(7):652－663.

Eckhardt, R.(1987), "Stan Ulam, John von Neumann, and the Monte Carlo method", *Los Alamos Science* (special issue):131－141.

Egger, D. J. et al(2020), "Quantum computing for finance: State of the art and future prospects", *IEEE Transactions on Quantum Engineering* 1:1－24.

Emms, D. et al(2009), "Graph matching using the interference of discrete-time quantum walks", *Image and Vision Computing* 27(7):934－949.

Farhi, E. et al(2000), "Quantum computation by adiabatic evolution", arXiv preprint quant ph/0001106.

Farhi, E. et al(2010), "Quantum state restoration and single-copy tomography for ground states of Hamiltonians", *Physical Review Letters* 105(19):190503.

Farhi, E. et al(2012), "Quantum money from knots", *Proceedings of the 3rd Innovations in Theoretical Computer Science Conference*, 8th－10th Jan., Cambridge, MA, United States.

Farhi, E. et al(2014), "A quantum approximate optimization algorithm", arXiv preprint arXiv:1411.4028.

Farhi, E. & H. Neven(2018), "Classification with quantum neural networks on near term processors", arXiv preprint arXiv:1802.06002.

Fedorov, A. K. et al(2018), "Quantum computers put blockchain security at risk", *Nature* 563(7732):465－467.

Feynman, R. P.(1982), "Simulating physics with computers", *International Journal of Theoretical Physics* 21(6):467－488.

Gamache, R. R. & R. W. Davies(1983), "Theoretical calculations of N2－broadened halfwidths of H2O using quantum Fourier transform theory", *Applied Optics* 22(24):4013－4019.

Gantz, J. & D. Reinsel(2012), "The digital universe in 2020: Big data, bigger digital shadows, and biggest growth in the far east", *IDC iView: IDC Analyze the Future* 2007(2012):1－16.

Gavinsky, D.(2011), "Quantum money with classical verification", 2012 IEEE 27th Conference on Computational Complexity, 26th－29th June, Porto, Portugal.

Gidney, C. & M. Ekerå(2021), "How to factor 2048 bit RSA integers in 8 hours using 20 million noisy qubits", *Quantum* 5:433.

Glasserman, P.(2003), *Monte Carlo Methods in Financial Engineering*, Springer.

Gomber, P. et al(2018), "On the Fintech revolution: Interpreting the forces of innovation, disruption, and transformation in financial services", *Journal of Management Information Systems* 35(1):220－265.

Gottesman, D. E. (1997), *Stabilizer Codes and Quantum Error Correction*, California Institute of Technology.

Grover, L. K. (1996), "A fast quantum mechanical algorithm for database search", *Proceedings of the 28th Annual ACM Symposium on the Theory of Computing*, 22nd－24th May, Philadelphia, Pannsylvania, United States.

Grover, V. & P. Ramanlal(1999), "Six myths of information and markets: Information technology networks, electronic commerce, and the battle for consumer surplus", *MIS Quarterly* 23(4):465－495.

Hajek, P. & R. Henriques(2017), "Mining corporate annual reports for intelligent detection of financial statement fraud - A comparative study of machine learning methods", *Knowledge-Based Systems* 128:139－152.

Han, K. et al(2011), "Information technology spillover and productivity: The role of information technology intensity and competition", *Journal of Management Information Systems* 28(1):115－146.

Han, K. H. & J. H. Kim(2000), "Genetic quantum algorithm and its application to combinatorial optimization problem", *Proceedings of the 2000 Congress on Evolutionary Computation*, 16th－19th July, California, United States.

Harrow, A. W. et al(2009), "Quantum algorithm for linear systems of equations", *Physical Review Letters* 103(15):150502.

Haven, E. E. (2002), "A discussion on embedding the Black-Scholes option pricing model in a quantum physics setting", *Physica A* 304 (3－4):507－524.

Herman, D. et al(2022), "A survey of quantum computing for finance", arXiv preprint arXiv:2201.02773.

Hull, J. (2003), *Options, Futures, and Other Derivatives*, Pearson.

Ilinski, K. (2001), *Physics of Finance: Gauge Modelling in Non-Equilibrium Pricing*, Wiley.

Kadowaki, T. & H. Nishimori(1998), "Quantum annealing in the transverse Ising model", *Physical Review E* 58 (5):53－55.

Kak, S. C. (1995), "Quantum neural computing", *Advances in Imaging and Electron Physics* 94:259－313.

Kerenidis, I. et al(2019), "Quantum algorithms for portfolio optimization", *Proceedings of the 1st ACM Conference on Advances in Financial Technologies*, 21st－23rd Oct., Zurich, Switzerland.

Kiktenko, E. O et al(2018), "Quantum-secured blockchain", *Quantum Science and Technology* 3(3):035004.

Landauer, R. (1961), "Irreversibility and heat generation of computing process", *IBM Journal of Research and Development* 5(3):183－191.

Lang, G. & P. Welzel(1996), "Efficiency and technical progress in banking: Empirical results for a panel of German cooperative banks", *Journal of Banking & Finance* 20(6):1003－1023.

Längkvist, M. et al(2014), "A review of unsupervised feature learning and deep learning for time series modeling", *Pattern Recognition Letters* 42:11－24.

Lessmann, S. et al(2015), "Benchmarking state-of-the-art classification algorithms for credit scoring: An update of research", *European Journal of Operational Research* 247(1):124－136.

Lin, M. et al(2013), "Judging borrowers by the company they keep: Friendship networks and information asymmetry in online peer-to-peer lending", *Management Science* 59(1):17－35.

Livshits, I. et al(2016), "The democratization of credit and the rise in consumer bankruptcies", *Review of Economic Studies* 83(4):1673－1710.

Lloyd, S. et al(2013), "Quantum algorithms for supervised and unsupervised machine learning", arXiv preprint arXiv 1307.0411.

Lloyd, S. et al(2014), "Quantum principal component analysis", *Nature Physics* 10(9):631－663.

Long, G. L. (2001), "Grover algorithm with zero theoretical failure rate", *Physical Review A* 64(2):022307.

Lu, J. et al(2022), "A new stock forecasting model by hidden quantum Markov models", Artificial Intelligence and Security: 8th International Conference, 15th－20th July, Qinghai, China.

Lutomirski, A. et al(2009), "Breaking and making quantum money: Toward a new quantum cryptographic protocol", arXiv preprint arXiv:0912.3825.

Lutomirski, A. (2010), "An online attack against Wiesner's quantum money", arXiv preprint arXiv:1010.0256.

Lutomirski, A. (2011), "Component mixers and a hardness result for counterfeiting quantum money", arXiv preprint arXiv:1107.0321.

Madsen, J. B. (2007), "Technology spillover through trade and TFP convergence: 135 years of evidence for the

OECD countries", *Journal of International Economics* 72(2):464－480.

Martin, A. et al(2019), "Towards pricing financial derivatives with an IBM quantum compute", *Physical Review Research* 3(1):013167.

McMahon, C. et al(2022), "Improving the efficiency of payments systems using quantum computing", arXiv preprint arXiv:2209.15392.

Merton, R. C.(1973), "Theory of rational option pricing", *Bell Journal of Economics & Management Science* 4(1):141－183.

Michael, F.(2010), "Quantum portfolios of observables and the risk neutral valuation model", arXiv preprint arXiv:1004.0844.

Milne, A. et al(2017), "Optimal feature selection in credit scoring and classification using a quantum annealer", 1Qbit White Paper, https://1qbit.com/whitepaper/optimal－feature－selection－in－credit－scoring－classification－using－quantum－annealer/.

Molina, A. et al(2012), "Optimal counterfeiting attacks and generalizations for Wiesner's quantum money", Theory of Quantum Computation, Communication, and Cryptography: 7th Conference, 17th－19th May, Tokyo, Japan.

Monras, A. et al(2010), "Hidden quantum Markov models and non-adaptive read-out of many-body states", *Applied Mathematical and Computational Sciences* 3(1):93－122.

Montanaro, A.(2015), "Quantum speedup of Monte Carlo methods", *Proceedings of the Royal Society A: Mathematical, Physical and Engineering Sciences* 471(2181):20150301.

Mosca, M. & D. Stebila(2010), "Quantum coins", *Error-Correcting Codes, Finite Geometries and Cryptography* 523:35－47.

Narayanan, A. & M. Moore(1996), "Quantum-inspired genetic algorithms", *Proceedings of IEEE International Conference on Evolutionary Computation*, 20th－22th May, Nagoya, Japan .

Orús, R. et al(2019a), "Forecasting financial crashes with quantum computing", *Physical Review A* 99(6):060301.

Orús, R. et al(2019b), "Quantum computing for finance: Overview and prospects", *Reviews in Physics* 4:100028.

Pastawski, F. et al(2011), "Unforgeable noise-tolerant quantum tokens", *Proceedings of the National Academy of Sciences* 109(40):16079－16082.

Patrick, R. et al(2018), "Quantum computational finance: Monte Carlo pricing of financial derivatives", *Physical Review A* 98(2):022321.

Peng, X. et al(2008), "Quantum adiabatic algorithm for factorization and its experimental implementation", *Physical Review Letters* 101(22):220405.

Philippon, T.(2019), "On Fintech and financial inclusion", NBER Working Paper, No. 26330.

Planck, M.(1901), "On the law of distribution of energy in the normal spectrum", *Annalen der Physik* 4(553):1－11.

Preskill, J.(2011), "Quantum computing and the entanglement frontier", arXiv preprint arXiv:1203.5813.

Racorean, O.(2015), "Quantum gates and quantum circuits of stock portfolio", arXiv preprint arXiv:1507.02310.

Rebentrost, P. & S. Lloyd(2018), "Quantum computational finance: Quantum algorithm for portfolio optimization", arXiv preprint arXiv:1811.03975.

Rebentrost, P. et al(2018), "Quantum computational finance: Monte Carlo pricing of financial derivatives", *Physical Review A* 98(2):022321.

Rich, S. & G. Barton(2014), "NSA seeks to build quantum computer that could crack most types of encryption", *The Washington Post*, Jan. 2.

Roget, M. et al(2021), "Quantum perceptron revisited: Computational-statistical tradeoffs", arXiv preprint arXiv:2106.02496.

Rosenberg, G.(2016), "Finding optimal arbitrage opportunities using a quantum annealer", 1QB Information Technologies Write Paper, http://1qbit.com/files/white－papers/1QBit－White－Paper－%E2%80%93－Finding－Optimal－Arbitrage－Opportunities－Using－a－Quantum－Annealer.pdf.

Rosenberg, G. et al(2016), "Solving the optimal trading trajectory problem using a quantum annealer", *Proceedings of the 8th Workshop on High Performance Computational Finance*, 15th Nov., Texas, United States.

Sakuma, T.(2020), "Application of deep quantum neural networks to finance", arXiv preprint arXiv:2011.07319.

Schaden, M.(2002), "Quantum finance", *Physica A: Statistical Mechanics and its Applications* 316(1－4):511－538.

Schuld, M. et al(2016), "Prediction by linear regression on a quantum computer", *Physical Review A* 94 (2):1—5.
Shor, P. W. (1997), "Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer", *SIAM Review* 41(2):303—332.
Simon, D. R. (1997), "On the power of quantum computation", *SIAM Journal on Computing* 26(5):1474—1483.
Stamatopoulos, N. et al(2019), "Option pricing using quantum computers", *Quantum* 4:291.
Sutherland, A. (2018), "Does credit reporting lead to a decline in relationship lending? Evidence from information sharing technology", *Journal of Accounting &Economics* 66(1):123—141.
Taddy, M. (2018), "The technological elements of artificial intelligence", in: A. K. Agrawal et al(eds), *The Economics of Artificial Intelligence: An Agenda*, University of Chicago Press.
Thakor, A. V. (2020), "Fintech and banking: What do we know?", *Journal of Financial Intermediation* 41(1):1—13.
Thiel, M. (2001), "Finance and economic growth—A review of theory and the available evidence", European Economy-Economic Papers 2008—2015, No. 158. European Commission.
Venturelli, D. & A. Kondratyev(2018), "Reverse quantum annealing approach to portfolio optimization problems", *Quantum Machine Intelligence* 1(1):17—30.
Vives, X. (2019), "Digital disruption in banking", *Annual Review of Financial Economics* 11:243—272.
Wang, G. (2017), "Quantum algorithm for linear regression", *Physical Review A* 96 (1):1—17.
Wiebe, N. et al(2012), "Quantum algorithm for data fitting", *Physical Review Letters* 109(5):1—5.
Wiesner, S. (1983), "Conjugate coding", *ACM Sigact News* 15(1):78—88.
Woerner, S. & D. J. Egger (2018), "Quantum risk analysis", *Nature Partner Journals* 5(1):1—8.
Wootters, W. K. & W. H. Zurek (1982), "A single quantum cannot be cloned", *Nature* 299(5886):802—803.
Wossnig, L. et al(2018), "A quantum linear system algorithm for dense matrices", *Physical Review Letters* 120(5):050502.
Yamamoto, Y. et al(2020), "Coherent Ising machines—Quantum optics and neural network perspectives", *Applied Physics Letters* 117(16):160501.
Zagoskin, A. M. (1986), *Applications and Speculations*, Cambridge University Press.

Applications of Quantum Computing to Economics and Finance

WANG Yong MENG Xiangjun SHEN Weiping
(Chinese Academy of Social Sciences, Beijing, China)

Abstract: In recent years, quantum computing, the speed of which far exceeds supercomputers, has been developed rapidly. Quantum computing has attracted wide attention in the society, and has exerted an important influence on economics and finance. This paper makes a systematic review of the development status, basic principles and applications of quantum computing in the economic and financial fields. It finds that the high efficiency of quantum computing can effectively improve the performance of economic forecasting, option pricing and portfolio selection, and can greatly improve the credit score and risk control model of commercial banks. However, it may bring certain security risks to digital currency. The paper further analyzes the mechanisms of quantum computing to optimize economic and financial operations, and discusses the potential channels through which quantum computing threatens economic and financial development. Finally, it summarizes and discusses the direction of quantum computing to promote the economic and financial development, and the future potential challenges in the development and application of quantum computing technology.

Keywords: Quantum Computing; Economic Forecasting; Option Pricing; Portfolio; Digital Currency

(责任编辑:刘洪愧)
(校对:刘新波)