

破解比特币加密核心门槛降至九百逻辑比特

41 篇 · 9 个来源 | PDF | 本期汇总免费阅读

本期目录

- 今日三件事
- 硬件前沿
- 算法与软件
- 产业与生态
- 学术前沿
- 今日影响
- 编辑点评

收录报道	41
信息来源	9
阅读时长	约 31 分钟

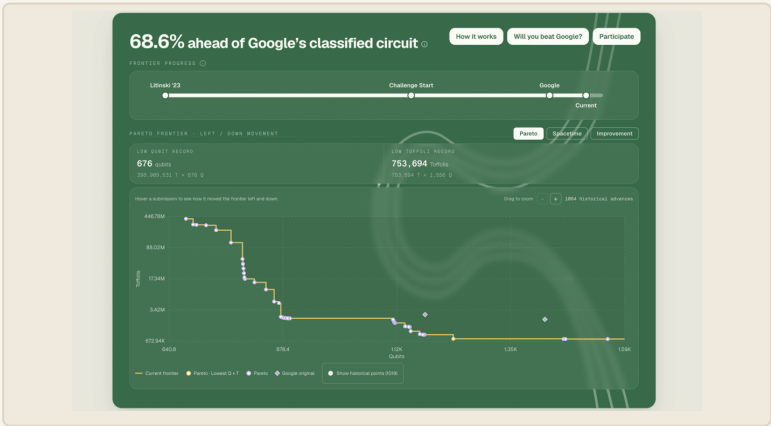
当前 S O T A

物理比特	1, 180
2Q 保真度	99. 99%
逻辑比特	96 LQ

量子硬件 SOTA 对照表 →

01 亮点

今日三件事

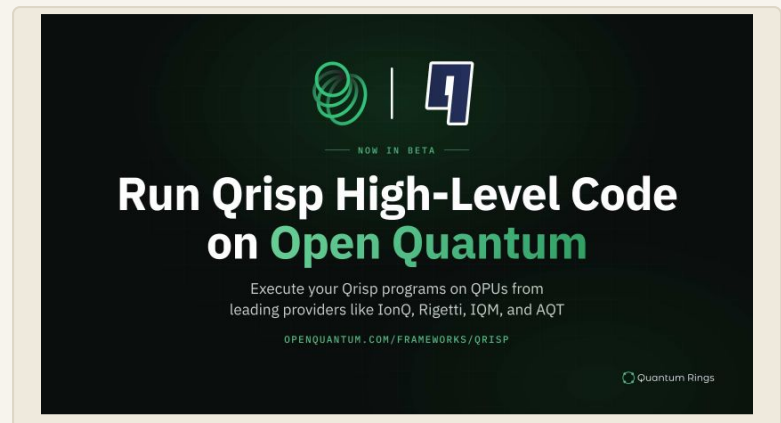


- 比特币公钥加密关键运算门槛降至九百逻辑比特**
全球基准测试榜单显示针对主流椭圆曲线的点加法电路所需规模首次压缩至900个逻辑量子比特以内且符合谷歌托佛利门开销预算^[3]——大幅拉近公钥破译与实体容错硬件的技术距离
- 摩根士丹利将离子阱龙头Quantinuum上调至超配评级**
华尔街顶级投行摩根士丹利正式上调Quantinuum股票评级至超配并列为旗下首选量子投资标的^[26]——确立高保真度全连接硬件在公开市场的估值溢价
- 东芝联手惠普企业落地抗量子网络安全专网**
惠普企业、东芝与SpeQtral联合发布面向关键基础设施的IPsec专用通信方案，将量子安全网络平台

集成至下一代企业级防火墙^[21]——打通商用网络安全硬件融合后量子密钥的落地链路

02 硬件

硬件前沿



容错纠错与超导路线

继此前理论模拟阶段后，最新硬件实验首次在物理芯片上完整运行魔态蒸馏（魔态：实现容错计算的关键量子态）协议，将输入逻辑量子比特中的错误率降低至原先的四十分之一（40倍降幅）^[2]。

技术含义上，这是该容错净化协议在全球物理实体芯片上的首次端到端闭环验证；对照当前超导与容错SOTA基线，目前行业最高误差压制因子为谷歌Willow芯片的表面码达到 $\Lambda \approx 2.1$ （码距 $d=7$ ），QuEra在自然杂志展示了96个纠错逻辑比特，而魔态制备长期以来占据容错计算超90%的物理资源；此次40倍硬件实测压制大幅缩小了算法与容错硬件的鸿沟，但距离通用实用化仍存在两大关键短板：一是全芯片纳秒级实时解码延迟尚未完全闭环，二是受限于超导芯片的两能级系统（TLS：材料缺陷

引起的相干损耗)波动,蒸馏过程中辅助比特的开销依然巨大。

格局影响方面,该进展直接降低表面码与级联纠错架构对物理比特数量的依赖,为IBM、谷歌以及计划在2029至2030年交付容错商用机的硬件制造商减轻了物理系统扩展压力^[2]。

瑞典查尔姆斯大学Next Labs、ConScience公司与新加坡国家量子联合铸造厂(NQFF)完成超导量子芯片QiB1的跨大洲联合验证,证实芯片在瑞典哥德堡与新加坡两地差异巨大的测试环境中往返运输并重新冷却后,其量子比特退相干时间与门操作参数完全保持稳定,未发生环境引发的性能衰退^[17]。

技术含义上,该项工作首次在跨国测试基准上建立了超导晶圆制造与远端装配的环境鲁棒性量化指标;对照超导SOTA基线中中位双比特门保真度(F_2Q 在99.5%至99.9%之间),本次测试证实了超导器件在物理运输层面的抗震与抗温变阈值,但全流程量产距离商业半导体标准仍缺少低温晶圆级全自动并行抽测规范。

格局影响上,这一成果为跨国分布式量子芯片代工、异地封装和全球客户现场交付模式扫清了质量风控疑虑,利好欧洲与亚洲的独立芯片制造服务商^[17]。

D-Wave系统公司在其Advantage2超导量子退火处理器上动用高达728个超导量子比特,成功执行了高阶拓扑绝缘体的三维模拟-数字混合量子模拟,通过自研的量子控制协议直接测量到局域边界态并提取出三维体相拓扑不变量^[15]。

技术含义上，这创下了固体物理中三维高阶拓扑相量子模拟的规模新高；对照超导通用门模型基线（如谷歌Willow的105比特及IBM Nighthawk的120比特），量子退火机在专一拓扑物态模拟上展现了728比特的规模优势，但由于其属于非通用哈密顿量演化机架，无法执行任意通用逻辑门；且系统仍需应对磁通噪声对有效退相干时间的侵蚀。

格局影响上，该进展进一步拓宽量子退火在复杂功能材料、拓扑超导体微观机制研究中的工业化模拟场景，对传统基于超算的高性能集群模拟形成互补^[15]。

光子与中性原子路线

科研人员采用确定性融合（光子融合：测量合并光子纠缠的机制）机制，在实验室内成功生成了具备多体纠缠特征的13光子量子图态，突破了此前长期停留在12个纠缠光子以内的技术瓶颈^[20]。

技术含义上，该实验刷新了全局多体纠缠光子数量与拓扑图态维度的公开纪录；对照光子路线SOTA基线（PsiQuantum在300毫米晶圆上测得双比特融合保真度为 $99.22\% \pm 0.12\%$ ），本成果在离散光子数上实现向上微幅推进，但在光子平台核心硬指标上依然缺少关键数据——所有保真度均以成功探测到光子为前提（属于条件保真度），完全未披露包含单光子源发射效率、片上波导插入损耗及超导纳米线单光子探测器（SNSPD）效率在内的端到端全链路损耗预算表。

格局影响上，该工作为基于测量的容错量子计算（MBQC）提供了更高维度的簇态资源基石，直接

利好PsiQuantum、加拿大Xanadu等光量子初创企业的架构演进^[20]。

室温与新型量子物理体系

SAXON Q研发团队构建的室温固态量子计算原型机利用3个量子比特运行格罗弗搜索算法

（Grover：量子无序数据库搜索算法），在脱离任何低温冷冻装置的常温常压环境下取得77.3%的目标态求解成功率^[27]。

技术含义上，这是首次在无制冷室温固态系统中验证了多比特量子搜索算法的数学有效性；对照低温主流SOTA基线（超导与离子阱单比特保真度超99.95%、双比特保真度普遍超99.5%），该系统77.3%的算法命中率相较于主流技术路线落后超一个数量级以上的精度误差；系统退相干时间极短且缺乏容错纠错编码支持，当前物理架构在可扩展性上仍存在明显上限。

格局影响上，该系统暂无法对通用数据中心量子计算形成替代，但在车载边缘探测、战术野外便携式计算等极端严苛场景中，确立了免稀释制冷架构的商业化雏形^[27]。

研究人员展示了一种利用惰性气体同位素原子自旋的新型室温量子磁传感原型方案，在完全摒弃液氦与低温真空系统的前提下，理论预期灵敏度潜在可达24 aT/ $\sqrt{\text{Hz}}$ （阿托特斯拉每根号赫兹：超微弱磁场测量单位）^[25]。

技术含义上，该灵敏度跨过了传统室温磁力仪的技术门槛，直接追平昂贵的低温超导量子干涉仪

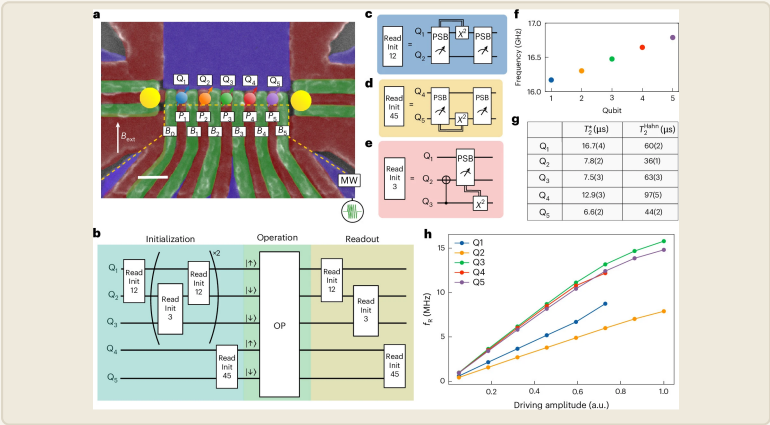
(SQUID) 主力测量区间；但距离工程化实用仍面临复杂动态环境下的主动磁场屏蔽补偿挑战。

格局影响上，该技术为高端生物医疗脑磁图、心磁图筛查设备的低成本移动化普及铺平道路，直接冲击传统低温医用影像仪器的供应链格局^[25]。

EeroQ联合创始人兼密歇根州立大学教授约翰内斯·波拉宁（Johannes Pollanen）在学术访谈中系统阐述了利用悬浮于超流氦薄膜之上的单个电子自旋构建量子比特的技术路线，强调借助成熟半导体硅制造工艺是实现百万量子比特扩展的唯一工程现实路径^[11]。

技术含义上，超流氦电子方案理论上兼具超导芯片的高时钟主频与捕获离子的极长相干时间，但目前该路线物理样机仍处于单比特与双比特的基础物理验证期，相较于已迈入数百比特及纠错验证期的超导与离子阱路线落后约一个代际。

格局影响上，该探讨向长期由超导和离子阱主导的硬科技风投机构展现了硅基杂化方案的潜在颠覆性，吸引长周期耐力资本关注^[11]。



密码学与安全编译

在最新设立的开源密码分析公开基准榜单中，针对主流区块链底层secp256k1椭圆曲线的点加法运算（签名生成与验证的核心数学步骤），全新优化的量子逻辑电路规模被成功压缩至900个逻辑量子比特以内，且整体门开销完全落在谷歌已公布的托佛利门（Toffoli：三比特受控非门）预算范围之内 [3]。

技术含义上，这是全球首次在满足工业级硬件约束（即门预算与特定拓扑）的前提下，将非对称加密关键攻击步骤的逻辑算力门槛拉低至三位数；尽管实现完整公钥破解仍需将点加法串联成离散对数求解整机线路，但在离散攻击算子的工程实现上跨过了关键分水岭。

格局影响上，该结果令传统加密金融网络（比特币、以太坊等）原本预估拥有10至15年的安全窗口期显著缩短，倒逼各大公链底层协议与核心托管机构在3至5年内全面加速后量子签名体系的硬分叉升级 [3]。

自动化程序合成与纠错优化

哈佛大学、Anthropic与QuEra计算公司的联合研发团队开发出一套基于深度自注意力机制的程序合成系统，在测试涵盖容错量子计算所需的8大核心基础运算原语时，自动化生成的优化电路相较于顶尖物理学家经验设计的人工基线，最高实现了达9100倍的硬件资源开销削减^{[13][35]}。

技术含义上，该系统直接生成结构完备的Python底层逻辑代码并自主完成门序列重构，在算子合成上首次证明高阶机器生成算法能够跨越人类数学直觉盲区，在非克利福德门（非Clifford门：实现通用容错计算不可或缺的高开销门操作）的综合优化上实现量级跨越。

格局影响上，该突破直接改写容错量子软件设计范式，极大压低了制药分子模拟与量子化学算法对物理硬件的严苛需求，使原本需要百万物理比特支撑的应用有望提前在万比特级硬件上跑通^{[13][35]}。

继此前发布纠错架构原型后，IBM研究院最新披露利用自主协同程序流水线对量子纠错硬件进行微架构拓扑搜索，在相同搜索预算下取得了较传统基线设计52倍的综合优化提速；在推理成本方面，基于前沿开源参数模型的配置仅消耗约26美元，较闭源商业模型的299美元成本低至约十一分之一（便宜11.5倍）^[30]。

技术含义上，该实验首次以精确财务数字证实了廉价开源基础模型流水线在复杂量子底层微架构设计中的工程可行性与超高投入产出比。

格局影响上，该方案打破了高精尖量子微架构设计仅限跨国巨头重金研发的壁垒，让中小科研团队与初创硬件公司能够以极低算力账单完成定制化纠错芯片设计^[30]。

量子软件创新团队Quantum X Labs发布LayerQake底层编译优化技术，在IBM三款现役主力超导芯片（ibm_fez、ibm_kingston及ibm_marrakesh）上进行实机压测，成功将多比特电路运行的累积误差最高降低至原先的二十分之一（相当于降低了21倍的噪声干扰）^[29]。

技术含义上，在无需改动物理硬件制冷与布线的前提下，纯粹通过软件层动态脉冲调度与串扰抵消重构了执行序列，显著拉伸了现有含噪声中等规模量子硬件的连贯计算深度。

格局影响上，该技术直接赋能租用IBM量子云平台的制药与材料模拟企业，使客户在现有物理硬件上即可运行更深层、更高保真度的化学模拟算法^[29]。

跨平台编译工具与应用范式

开源机构Open Quantum正式发布Qrisp高阶量子开发框架的硬件直通原生模块，支持将高阶算法一键编译并直接在IonQ、Rigetti、IQM以及AQT等多家厂商的异构物理硬件上执行，开发者无需针对各厂商底层门集编写汇编级代码^[16]。

技术含义上，框架内置自动化比特分配与拓扑路由算法，在应用层软件与异构底层硬件之间架设起标准化编译中间件，消除了跨物理架构迁移的移植损耗。

格局影响上，该项目削弱了头部单点硬件厂商在底层软件生态上的专有绑定权，促进全行业量子应用向平台无关的开源标准化方向收敛^[16]。

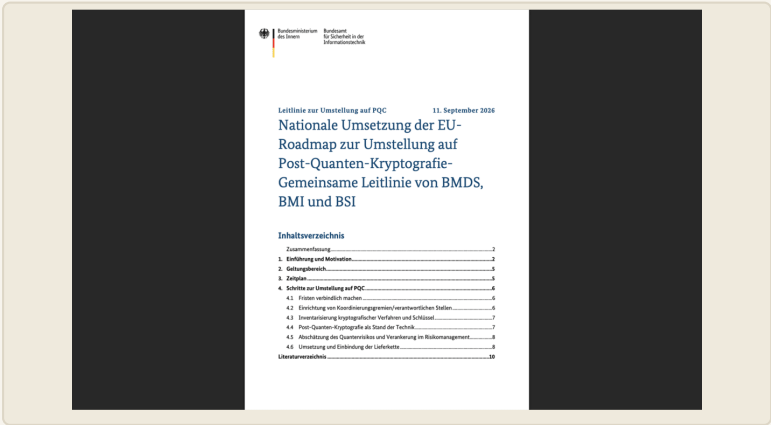
基普量子（Kipu Quantum）在QuEra公司研制的256比特Aquila中性原子量子处理器上，成功调度200个中性原子阵列进行模拟量子特征提取，在分子毒性分类基准任务中测得的特征分辨表现全面超越了传统算法模型^[19]。

技术含义上，这是首次在200比特以上的中性原子硬件上实测验证了模拟量子动力学在生化多维特征映射中的算力增益，避开了严苛的全局门保真度瓶颈。

格局影响上，该工作为中性原子计算硬件打开了除纯物理模拟之外的医药初筛商业大门，加速生物医药企业与量子初创公司的商用概念验证落地^[19]。

04 产业

产业与生态



资本市场与产业政策

华尔街国际投资银行摩根士丹利（Morgan Stanley）正式将离子阱量子硬件领军企业 Quantinuum 的投资评级由平配上调至超配，并明确将其确立为该行在整个量子计算领域的首选投资标的^[26]。

商业含义上，摩根士丹利在研报中指出，当前公开二级市场尚未充分认知 Quantinuum 的商业内在价值。

格局影响上，这一评级重新树立全球资本对量子硬件企业的估值标尺，驱动风险投资与公开市场资金加速流向兼具高保真度与容错纠错工程能力的头部阵营^[26]。

继此前欧盟框架发布后，德国内政部、数字化部与联邦信息安全局正式颁布国家级落地指南，强制要求政府机构、核心商业体系与关键基础设施必须在 2030 年前彻底完成高风险系统的后量子加密替换，并增设 2026 年底的中期审查节点，要求各实体必须在 2026 年底前明确责任人并完成首次密码资产清查^[4]。

商业含义上，合规要求的刚性化将倒逼德国乃至全欧洲的企业级 IT 支出结构发生倾斜，密码资产清查与自动化发现软件将成为未来 24 个月最确定的企业级采购支出。

格局影响上，该政策直接利好提供自动化密码资产梳理与抗量子算法迁移服务的网络安全厂商，对在德运营的跨国金融与工业实体构成实质性合规问责压力^[4]。

新加坡网络安全局（CSA）公布国家扶持细则，对受其监管并被勒令在2031年前完成抗量子改造的关键信息基础设施运营机构，由国家财政承担高达70%的迁移试点项目改造成本^[5]。

商业含义上，通过国家财政真金白银兜底前期试错成本，将极大消除金融机构与公用事业企业对早期技术路线不确定性的观望情绪。

格局影响上，该举措加速新加坡确立亚太地区后量子金融安全枢纽地位，为全球其他金融监管机构提供了财政补贴推动合规迁徙的政策蓝本^[5]。

欧洲量子工业财团（QuIC）向欧盟执行机构提出正式诉求，要求在所有成员国内推行全流程电子化审批并强制公开牌照审批处理周期，同时呼吁将韩国纳入欧盟两用物项通用出口许可EU001框架，以避免成员企业在繁琐审批中流失亚太客户订单^[8]。

商业含义上，诉求反映出欧洲量子产业链在上游核心零部件与先进测控系统上的商业出海焦虑，出口管制造成的交付拖延正侵蚀欧洲本土硬件厂商的国际市场份额。

格局影响上，若欧盟采纳诉求，将显著缩短亚太地区实验室与商业客户采购欧洲高精度稀释制冷机及测控电子元件的供应链交期^[8]。

行业落地与跨界协同

信息技术基础设施巨头惠普企业（HPE）、东芝与新加坡量子安全通信商SpeQtral联合推出面向关键信息基础设施与政府部门的量子安全网络解决方案，将东芝QSN平台与惠普下一代网络防火墙硬件

实现互联，在IPsec VPN通道中引入动态抗量子密钥材料^[21]。

商业含义上，方案打通了量子保密通信专用硬件与主流数据中心网络设备之间的物理协议壁垒，将前沿量子密钥分发与后量子密码以即插即用方式集成进主流IT架构。

格局影响上，该合作拉低关键部门部署量子通信保障的工程门槛，加速传统网络安全基础设施向后量子纵深防御演进^[21]。

托管全球约12%流通比特币的加密资产托管服务商Coinbase于10月13日针对比特币抗量子签名方案明确列出三大硬件系统准入诉求：必须原生支持多方安全计算（MPC：多方联合签名技术）、支持硬件安全模块（HSM）物理存储，以及采用无状态签名模式，并明确指出多方安全签名的适配是全行业最难攻克的瓶颈^[9]。

商业含义上，作为管理超千亿美元资产的托管机构，Coinbase的需求直接代表了机构级托管资金的底线风控要求，任何无法兼容多方联签的算法提案都将被机构托管系统直接否决。

格局影响上，这为比特币社区与密码学界的后量子升级路线设定了严格的工业级筛选标准，防止技术提案脱离金融实务脱节演进^[9]。

西班牙加泰罗尼亚生物工程研究所（IBEC）在巴塞罗那主持召开欧洲量子医疗影像联盟项目推进会，全面展示了NVision公司的量子增强分析软件，共同推进总预算达830万欧元的医疗研发项目，旨在

利用量子传感器与增强算法提升核磁共振成像（MRI）对早期疾病的诊断分辨率^[28]。

商业含义上，项目标志着量子传感与前沿算法正式切入高壁垒的体外与体内医学影像早筛赛道，打通了从基础物理至临床影像设备的商业转化通路。

格局影响上，该进展推动传统高场强MRI设备通过量子软件与超极化技术实现性能跃升，加速肿瘤及代谢疾病超早期影像早筛的技术渗透^[28]。

美国知名联邦研发智库MITRE发布针对八大主流企业级IT技术类别的后量子就绪度审计，数据显示密钥交换协议虽已在5个类别进入通用发布阶段，而后量子数字签名仅在2个类别落地；且目前市场上尚未存在任何获得FIPS（联邦信息处理标准）正式合规认证的企业级技术产品，也无任何可商用采购的后量子硬件可信平台模块（TPM）芯片^[6]。

商业含义上，审查揭示了当前企业安全宣传与真实硬件供应链之间的巨大鸿沟，企业即便有改造预算，在物理芯片与硬件根信任层仍面临无货可买的尴尬境地。

格局影响上，该报告预警全球金融系统与政府机构，若硬件半导体厂商无法在2027年前实现后量子TPM的规模量产，2030年的全面迁移大限势必面临实质性延期^[6]。

以太坊二层扩容网络Starknet的开发方StarkWare在其治理论坛向质押节点发起公开征询，探讨是否应因以太坊主网应对量子威胁行动缓慢而研究脱离以太坊主网；社区测算显示脱离将面临巨额流动性断裂成本，且Starknet用户当前最直接的量子暴露

面在于其本地椭圆曲线公钥签名，该环节并不受制于以太坊基础层^[7]。

商业含义上，探讨反映出去中心化金融生态对量子威胁响应周期的深层焦虑，二层网络试图通过架构自主化摆脱底层主网的技术滞后拖累。

格局影响上，这一争论促使以太坊核心开发者团队重新审视其抗量子路线图的排期优先级，加速智能合约生态的账户抽象与密码敏捷化改造^[7]。

越南科技巨头FPT集团与法国中性原子量子公司Pasqal拟建立战略合作伙伴关系，于北京时间10月12日向越南副总理胡国勇当面汇报国家级量子计算发展规划^[23]。

商业含义上，欧洲成熟中性原子硬件厂商通过绑定发展中国家IT龙头，以政府合作方式开辟新兴市场，实现技术资产出海。

格局影响上，该合作为东南亚国家跳过昂贵的超导硬件早期摸索、直接依托中性原子算力底座切入区域算力基建提供了示范案例^[23]。

印度马尼帕尔理工学院班加罗尔分校正式启用量子创新中心（Q-HUB@MAHE），引进了由QuantrolOx公司开发的VIDYAQAR开放架构稀释制冷系统，首期具备25个超导比特测控能力并已规划向千比特级平滑升级，计划首期培养100名全栈量子工程师^[18]。

商业含义上，印度国家量子任务专项资金正在快速向头部工科院校渗透，通过开放式模块化采购构建自主可控的底层研发实操基地。

格局影响上，该中心加速南亚次大陆在量子测控与硬件工程化领域的人才储备，逐步改变全球量子工程人员供给版图^[18]。

马来西亚砂拉越人工智能中心（SAIC）与IBM马来西亚公司达成战略合作，计划在东马来西亚设立该国首个量子安全创新中心，旨在提升关键信息资产的网络韧性并推动区域数字化主权^[22]。

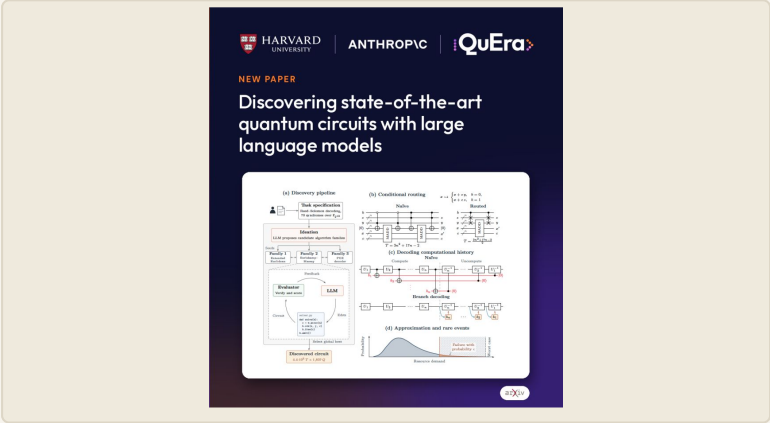
商业含义上，IBM通过输出成熟的抗量子咨询与算法框架，进一步扩大其在东南亚政府与能源枢纽市场的企业级生态版图。

格局影响上，该合作带动东盟次区域关键基础设施防御体系提早对标国际后量子密码规范^[22]。

由鲍勃·苏托尔（Bob Sutor）与布赖恩·西格尔瓦克斯（Brian Siegelwax）联合策划的第三届纽约 Quantum+AI（Q+AI）峰会将于北京时间10月下旬在纽约市开幕，大会汇集超80位全球行业领袖，重点设立后量子密码（PQC）与硬件落地产业专属研讨分论坛^[1]。

商业含义上，会议筹备显示出后量子密码合规与前沿算力融合已成为跨国科技巨头与华尔街金融机构高管必须直面的年度核心议题。

格局影响上，该活动进一步强化北美在后量子产业规范、资本对接与顶层政策倡导上的纽带作用^[1]。



拓扑物理与材料理论

麻省理工学院物理系研究人员开发了一种专用的自注意力机制多体神经网络，在强朗道能级混合极端条件下对复杂量子多体薛定谔方程进行数值求解，首次从微观物理层面确证了反Pfaffian拓扑相态（拓扑态：内建抗噪能力的物质相态）的真实存在 [14]。

技术含义上，该成果成功化解了凝聚态物理界数十年来围绕分数量子霍尔基态拓扑属性的激烈争论；更关键的是，这一拓扑序在单层二硒化钨（WSe2）与半导体异质结量子阱中获得了明确的材料映射参数，为人工合成内建抗退相干特性的非阿贝尔拓扑量子比特提供了精确微观蓝图。

格局影响上，研究从基础理论上提振了拓扑量子计算路线的可行性，为微软等长期坚持拓扑路线的研发机构提供了寻找马约拉纳零能模之外的全新二维材料体系选择 [14]。

密码审计与前沿算法综述

密码学研究团队开发出一种结合零知识证明、联邦查询、安全聚合与私有集合求交（PSI：不泄露原始数据即可求交集的技术）的协同评估机制，使金融监管机构能够在完全不收集企业原始软件物料清单的前提下，自动化测算出整个行业各关键节点的密码学暴露敞口^[10]。

技术含义上，该机制化解了欧盟法规推行过程中「监管合规需要审计软件细节」与「企业担心商业源代码核心资产泄露」之间的结构性矛盾，实现了密码学敏感信息的去中心化隐匿审计。

格局影响上，方案大幅降低金融系统与国防工业落实后量子合规自查的阻力，为全球监管机构提供了一套兼顾隐私保护与系统性风险宏观监测的标准工具箱^[10]。

学者刘宏川系统梳理并深度评估了全球119篇高水平研究成果，将自适应组合优化领域的算法演进精确划分为三类前沿范式：经典算法辅助量子优化、量子算法加速经典模型以及双向协同优化，结论明确指出当前通过经典深度网络辅助量子参数优化的路径收效最为显著，而反向赋能则受制于现有硬件的保真度瓶颈^[12]。

技术含义上，综述为业界厘清了长期以来在量子优化优越性上的认知误区，明确指出在纠错通用量子计算机成熟之前，以经典计算为主干、量子芯片为特定加速协处理器的混合计算才是最具落地潜力的现实形态。

格局影响上，梳理为关注量子优化的产业资本与企业研发团队提供了客观的选型坐标系，防止盲目投入无法落地的纯量子退火或变分算法^[12]。

连续变量与光子量子态

科研人员研制出一种基于集成三光子克尔参量振荡器（KPO：利用三阶非线性效应产生叠加态的光学器件）的固态光子芯片，在微纳波导结构中成功观测并确认了类似薛定谔猫态的量子叠加特征，实测证实了芯片系统内部的高保真度量量子相干性^[32]。

技术含义上，芯片在片上微纳尺度实现了高阶非线性非高斯态的相干制备，为基于玻色编码和连续变量的硬件容错架构补充了关键的紧凑型微观发生源。

格局影响上，实验为从事集成光量子芯片研发的初创企业拓宽了量子态制备技术树，有望在更小芯片面积内集成更多有效信息容量^[32]。

研究团队利用成熟的离子阱技术结合高相干光子接口，在两处物理隔离的远程网络节点之间实现了纠错量子比特的跨空间量子纠缠，测得远程纠缠态的保真度超过95%^[24]。

技术含义与SOTA对比上，该实验成功跨越了长久以来困扰分布式量子互联的量子比特退相干瓶颈；对照内部单机离子阱门保真度99.99%的SOTA水准，跨节点95%的保真度已处于国际分布式纠缠领先区间，但距离容错分布式集群所需的99%以上门槛仍存在近一个数量级的误差落差，且低光子耦合收集效率导致的低重复率问题仍待突破。

格局影响上，工作为下一代基于模块化拼接的超大规模量子计算机以及跨数据中心量子保密骨干网的工程架构提供了强有力的物理实验支持^[24]。

牛津大学物理系实验团队利用双元素冷原子构建分布式量子网络，通过铯原子实现对光子的高效耦合传输，同时利用钙原子充当长寿命量子存储载体，成功将两处独立空间之间的共享量子纠缠维持时间延长至10秒以上，并成功演示了多达4个原子的跨节点相干态^[31]。

技术含义与SOTA对比上，团队将跨节点量子纠缠的存储寿命从以往毫秒级量级提升了两个数量级以上，有效化解了光子传输衰减与存储退相干不能兼得的矛盾；不过双元素系统对激光波长与锁相控制的要求极高，目前纠缠分发的通信吞吐率仍有待提升。

格局影响上，该突破为长距离量子中继器与广域量子通信网络搭建扫除了核心存储寿命障碍，直接利好国家级量子保密通信骨干工程的方案论证^[31]。



1 数字加密与区块链产业：公钥密码被破译预期步步逼近，倒逼多方联签技术紧急重构^[3]^[9]^[7]

谁受影响：持有数千亿美元资产的加密货币交易所、区块链公链基金会、数字资产托管机构及个人投资者。

什么变了：破解比特币与以太坊公钥加密关键运算的逻辑量子比特门槛首次被压至900个以内，且满足谷歌硬件门预算^[3]；Coinbase明确披露现有后量子方案难以适配多方安全计算（MPC）硬件^[9]，以太坊二层网络Starknet甚至开始研判脱离主网自保^[7]。原本被认为至少10年后才到来的量子威胁，已演变为未来3年内必须落地的工程升级大考。

下一步盯什么：密切盯梢以太坊基金会与比特币开发者社区对无状态后量子签名提案的审核动向，以及主流硬件安全芯片厂商何时推出原生兼容后量子多方签名的物理模块。

1 企业级IT合规与信息安全：政策大限与硬件供应链产生断层，倒逼安全预算投向资产审计^[4]^[5]^[6]

谁受影响：跨国银行、能源电信等关键基础设施运营机构、企业首席信息安全官（CISO）。

什么变了：德国划定2026底资产清查死线与2030大限^[4]，新加坡直接出资70%补贴关键系统改造^[5]；然而MITRE最新审查显示，全行业目前没有任何一款技术获得FIPS合规认证，商用后量子TPM硬件模块供应更是交出白卷^[6]。合规强制力与物理硬件缺位形成巨大落差。

下一步盯什么：紧盯美国NIST正式颁布首批商用FIPS算法认证的精确时间表，以及英飞凌、意法半导体等芯片巨头推出商用后量子TPM物理模块的量产交付节点。

1 量子硬件工程化与纠错研发：深度程序合成全面接管微架构设计，研发周期由年级压至小时级^{[13] [30]}

谁受影响：量子芯片微架构设计师、纠错码算法研发人员、EDA自动化软件开发商。

什么变了：哈佛与Anthropic等借助程序合成将电路资源开销骤降达9100倍^[13]，IBM以26美元推理成本取得52倍硬件架构优化加速^[30]；以往依赖顶尖物理学家直觉人工推导纠错微架构的设计范式正在被彻底颠覆，开源低成本程序合成正在成为最强大的工程利器。

下一步盯什么：观察自动化生成的复杂纠错电路在真实超导与中性原子物理芯片流片测试中的保真度

表现，以及Qrisp等跨平台编译框架对自动化生成代码的原生支持进展^[16]。

1 二级市场投资与资本配置：华尔街打破观望确立超配地位，估值锚点转向全连接与保真度^[26]

谁受影响：关注前沿科技的对冲基金、一级市场硬科技风投、量子计算上市与拟上市企业管理层。

什么变了：摩根士丹利正式上调Quantinuum至超配评级并列为行业首选^[26]；标志着国际主流投行对量子赛道的估值逻辑发生质变——不再单纯迷信虚高的物理比特数字，而是全面锚定全连接物理比特保真度（如Helios达99.921%）与容错逻辑比特的工程兑现能力。

下一步盯什么：持续关注Quantinuum筹备独立IPO的分拆上市进程，以及华尔街各大投行对超导与离子阱各家领军企业保真度资产的重估报告。

07 编辑

编辑点评

量子算力演进正呈现出一场鲜明的非对称加速。在破译端与算法层，理论推演和优化工具正在以前所未有的速度侵蚀传统安全防线——关键数学算子的逻辑比特开销正被精准压入百位量级，算法的工程实现与物理机器的结合点正在不断前移。然而，在防御端与实体工业界，我们却看到了一场迟滞的行军：尽管国家层面的强制合规期限日益紧迫、财政补贴真金白银下达，但底层的硬件安全模块、工业级多方联签方案以及端到端的芯片级信任根却面临

严重的供应链空白。这种算法进攻走在工程防御之前的剪刀差，正给全球数字资产与关键信息基础设施敲响警钟。

与此同时，量子研发本身的底层工具链正在经历深刻的工业自动化革命。过去几十年，量子物理学家依靠手工推导、试错拼接纠错线路与微架构的传统手工作坊模式，正被基于深度自注意力网络和多智能体协同流水线的程序合成技术彻底取代。几十美元的计算成本就能换来数十倍的架构优化加速与成千上万倍的资源开销削减。这意味着，量子计算正在从物理学家在实验室寻找物理现象的探索阶段，全面跨入以现代化自动化软件重构物理芯片工程实现的成熟工业期。谁能率先将先进自动化代码生成工具与高保真度物理硬件闭环打通，谁就将掌握通往容错量子霸权的终极钥匙。

参考资料

[1] The New Quantum Era with Sebastian Hassinger	[5] Singapore Will Pay Up to 70% of Quantum-Safe Migration Pilots, Critical Infrastructure First
[2] Quantum magic state cleanup cuts errors 40-fold in first successful hardware test	[6] MITRE Rated Eight Enterprise Technologies on Post-Quantum Readiness. Key Exchange Is in General Release in Five, Signatures in Two.
[3] A Key Step of a Quantum Attack on Bitcoin and Ethereum Now Fits in Under 900 Logical Qubits Within Google's Gate Budget	[7] Starknet Asks Its Stakers Whether to Research Leaving Ethereum Over Quantum Risk
[4] Germany Sets a 2030 Post-Quantum Target for High-Risk Systems in Government, Business and Critical Infrastructure	

- [8] Europe' s Quantum Industry Association Asks the EU for Faster Export Licensing
- [9] Coinbase, Which Says It Holds About 12% of All Bitcoin, Sets Out What It Needs From Bitcoin' s Post-Quantum Signatures. Its Request for Multi-Party Signing Is the Hardest to Meet.
- [10] Supervisors Can Measure a Sector' s Cryptographic Exposure Without Collecting Anyone' s Inventory
- [11] Podcast with Johannes Pollanen, Co-founder of EeroQ and a Professor of Physics at Michigan State University
- [12] Review Evaluates AI and Quantum Computing Paradigms for Adaptive Combinatorial Optimization
- [13] RIKEN Demonstrates High-Fidelity Simultaneous Control of Silicon Spin Qubits Above 99.9% Threshold
- [14] Harvard, Anthropic, and QuEra Use LLMs to Discover Quantum Circuits with Up to 9,100x Lower Resource Costs
- [15] MIT Physicists Use First-Principles AI to Resolve Non-Abelian Anyon Order at Strong Landau Level Mixing
- [16] D-Wave Demonstrates 3D Analog-Digital Quantum Simulation of Higher-Order Topological Insulators Using 728 Qubits
- [17] Open Quantum Launches Native Qrisp Integration for High-Level QPU Execution Across IonQ, Rigetti, IQM, and AQT Hardware
- [18] Chalmers Next Labs, ConScience, and NQFF Validate Superconducting Qubit Chip Stability Across International Testbeds
- [19] MIT Bengaluru Inaugurates Q-HUB@MAHE and Deploys QuantroIOx' s Open-Architecture VIDYAQAR Quantum System
- [20] Kipu Quantum Demonstrates Neutral-Atom Quantum Feature Extraction for Molecular Toxicity Classification on QuEra Hardware
- [21] Researchers Entangle 13 Photons to Build Larger Quantum Graphs
- [22] Toshiba, SpeQtral and HPE secure data with quantum-safe VPNs
- [23] Sarawak AI Centre and IBM will build Malaysia' s first quantum-safe hub
- [24] FPT and Pasqal Plan Quantum Computing Push in Vietnam
- [25] Yang Ming Chiao Tung Team Proposes Loss-Tolerant QKD Via Time Bins

[26]

Researchers Generate Remote Entanglement at 95% Fidelity

[27]

Room-temperature quantum sensor skips the need for cryogenic cooling

[28]

Morgan Stanley picks Quantinuum as its top quantum stock

[29]

SAXON Q’ s three qubits hit a 77% target rate at room temperature

[30]

Anderon releases a design kit for superconducting quantum chips

[31]

Catalonia bioengineering institute showcases NVision Quantum software for MRI data

[32]

LayerQake at Quantum X Labs cuts qubit errors by up to 21x on IBM chips

[33]

IBM achieves 52x design speedup with AI agents tackling quantum error correction

[34]

Strontium links atoms, calcium preserves entanglement for longer

[35]

Cat-like quantum states confirmed in a three-photon chip

[36]

Qubit Community Weekly Newsletter #87

[37]

Plants move to get away from their decaying brethren

[38]

Anthropic’ s Claude Designs Leaner Quantum Circuits, Reducing Resources Needed for Key Calculations

[39]

Robert Wille (Munich Quantum Software Company): Quantum software needs design automation, not just algorithms

[40]

Guest Post: AI Infrastructure Investment and the Future of Quantum Computing

[41]

Quantum Computing Weekly Round-Up: Week Ending October 17, 2026

量子研究内参

全部期数 · 周刊深度解析 · 每日快报 → qbitbrief.com

FOR RESEARCH REFERENCE ONLY

配图源自所引论文与新闻稿；如引用不规范，请联系编辑部删除。