

比特币备战量子破解万亿加密资产面临换锁

42 篇 · 17 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 42

信息来源 17

阅读时长 约 17 分钟

当前 SOTA

物理比特 1,180

20 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

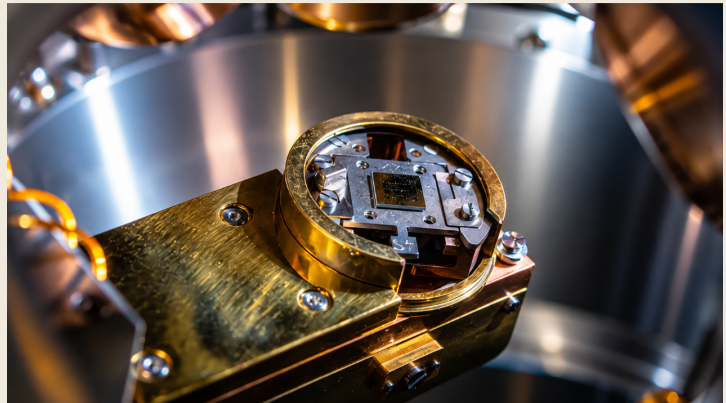


- 1 **IBM百比特芯片控制量子混沌** IBM联合罗格斯大学利用数千次中途重置（在计算中测量并清零）在100个超导量子比特芯片上实现混沌到受控动力学转换^[12]——开辟多体动力学控制路径，但距纠错仍有代差。
- 2 **英政府九百万英镑资助量子传感** 英国创新署向Infleqtion拨付900万英镑将中性原子射频测向系统推进至机动车载实装^[3]^[33]——加速中性原子传感从实验室迈入万亿国防实战。
- 3 **D-Wave携手美代工厂签多年制造长约** D-Wave与美国本土代工厂SkyWater签署多年制造协议

以继续特种半导体制造^[35]——打通全美超导芯片自主代工与商业量产闭环。

02 硬件

硬件前沿



超导芯片与材料工艺

IBM联合罗格斯大学在100个超导量子比特处理器上，通过执行数千次电路中途重置（在计算中测量并清零），成功将多体量子系统的演化从混沌发散状态驱动并锁定至受控的定态动力学区间^[12]。【对照超导SOTA基线】该实验展示了非么正（不保持总概率为一）耗散操作对相空间发散的压制能力，但其物理机制绝非量子纠错；当前超导纠错金标准为谷歌Willow系统验证的低于阈值表面码（一种网格结构纠错码）（误差压制因子 $\Lambda \approx 2.1$ ，码距 $d=7$ ），而本实验完全不包含综合征测量（测辅助比特以排查错误）与逻辑比特纠错闭环^[12]。该技术为含噪声量子硬件模拟非平衡态凝聚态物理提供了新手段，但在通用容错计算路线上无法替代纠错

码，预计未来3至5年主要局限于物理学术课题研究^[12]。

美国费米国家加速器实验室领衔的超导量子材料与系统中心（SQMS）完成了一项跨尺度材料微观表征研究，将超导三维谐振腔及跨导量子比特（抗电荷噪声超导比特）的晶界微观缺陷与微加工工艺特征精确关联至器件退相干波动^[2]。【对照超导SOTA基线】超导路线头部器件的能量弛豫时间（激发态寿命衰减时长）（ T_1 ）处于100至500微秒区间（如谷歌Willow达到约100微秒），但行业普遍面临两能级系统（材料缺陷微观吸收体）导致的2至3倍时序随机波动；该研究从微观界面氧化层厘清了高频损耗来源，为突破500微秒相干瓶颈提供了明确工艺改进路径^[2]。这一工艺发现将直接影响IBM、IQM等整机厂的薄膜生长与洁净室规范，预计在2年内推动超导上游高纯靶材与晶圆加工标准的更新^[2]。

离子阱与混合架构

继北京时间2026年10月10日报道后，第三方技术评估进一步拆解了离子阱厂商IonQ利用光纤链路连接单颗铯离子与金刚石硅-空位（金刚石中发光点缺陷）色心存储器的实测数据，其纠缠分发速率为每秒1000次，纠缠保真度（实际态与理想态吻合度）为88%^[11]。【对照离子阱与互连SOTA基线】虽然每秒1000次的速率达到了此前囚禁离子间最快光子互连纪录的4倍，但88%的保真度远落后于离子阱双比特门SOTA（IonQ自身EQC原型的99.99%与Quantinuum商用全比特对99.921%），亦落后于光子互连SOTA（PsiQuantum的42米光纤互连保真

度99.72%)；更关键的是，IonQ自身学术论文论证指出，构建分布式容错计算网络所需的模块间纠缠速率在每秒1万至10万次之间，当前硬件实测值落后理论阈值10至100倍^[11]。该差距表明光纤互连的分布式离子阱算力集群无法在短期内取代单芯片扩展，多芯片拼接路线至少还需5至7年的光学工程攻坚^[11]。

国际科研团队利用囚禁离子量子模拟器成功模拟了高能物理中的胶子弦断裂（夸克禁闭解除过程）非微扰动态演化^[10]。该实验利用离子链的全连接库仑相互作用构建规范场模型，验证了极端高能物理实验在量子硬件上进行实时动力学重构的可行性^[10]。成果推动量子模拟加速渗透至欧洲核子研究中心等粒子物理重地，预计在3至5年内成为强关联粒子模拟的辅助验证工具^[10]。

光量子与通信链路

欧洲航天局（ESA）正式确认达成空间通信预定指标，在1560纳米电信波段实现了偏振纠缠光子（偏振关联的光子对）对产生速率突破1吉赫兹（每秒10亿对）的技术门槛^[21]。【对照光子SOTA基线】1吉赫兹产生速率使星地量子通信发射端吞吐量提升至此前百兆赫兹量级实验源的近10倍，全面适配高带宽量子密钥分发（基于量子态的分发密钥）与分布式算力并网需求；但在接收端，全系统端到端损耗依然受制于探测端超导纳米线单光子探测效率（基线要求 $\geq 95\%$ ）与大气吸收衰减^[21]。该技术跨过了空间高速保密通信发射端工程门槛，将直接支撑欧洲下一代量子卫星星座部署，预计2028年前后开启欧洲泛大陆轨道密钥分发业务验证^[21]。

荷兰量子研发机构QuTech将一套关键量子硬件实验测试平台整体迁移并交付至德国卡尔斯鲁厄理工学院（KIT）实验室^[22]。该跨国搬迁标志着欧洲在拓扑与超导杂化量子器件的科研协同从概念走向跨国设备共享，缩短了德荷两地新型器件验证周期^[22]。

中性原子与拓扑物态

科研人员在《Quantum》期刊发表成果，利用光镊阵列精确排列的里德伯原子（外层电子高激发原子），在任意拓扑空间网络结构上提出了连续时间量子行走（量子态在网络中扩散）模拟的理论实现方案^[19]。【对照中性原子SOTA基线】该方案突破了传统固定光学晶格的几何维度限制，利用中性原子位点动态重排能力实现了非欧几里得空间拓扑构造；但受限于中性原子平台1至10赫兹的循环重复率短板，更大规模图模拟的耗时仍较长^[19]。该进展为社交网络社群发现、交通物流路径规划等图论难题提供了全新的量子拓扑演化测试方案^[19]。

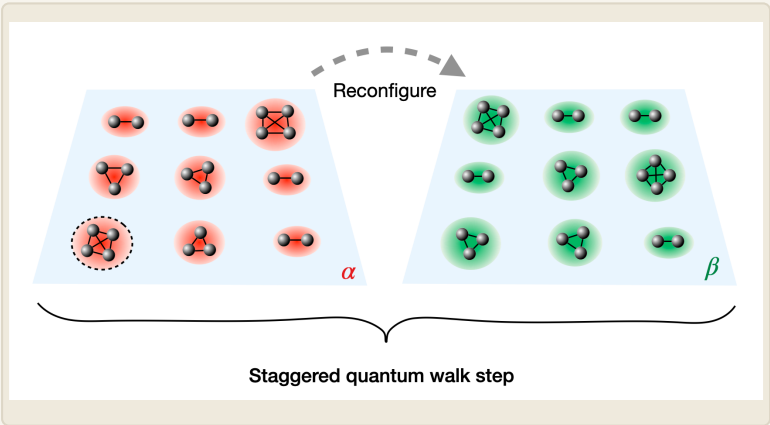
材料科研人员通过开发“地毯式”表面外延生长新工艺，成功制备出大面积且厚度均一的二维拓扑绝缘体（体绝缘但边缘导电材料）新型薄膜^[6]。该材料具有体态绝缘而边缘无耗散自旋单向传导的特性，为制备高稳定性马约拉纳费米子拓扑量子比特提供了高质量物理基底，预计在未来3到5年内助力拓扑硬件路线攻克材料均匀性难题^[6]。

物理学者利用层状拓扑材料制成扫描隧道显微镜探针，在原子级空间分辨率下首次直接捕获到二维交替磁性（零净磁矩自旋劈裂磁序）的电子态特征^[8]。该技术填补了原子尺度自旋局域探测的仪器空

白，为开发新型自旋量子存储器与超低功耗无耗散自旋器件开辟了新的观测工具体系^[8]。

03 算法

算法与软件



发表于《npj量子信息》的理论研究提出了名为“镜像子空间对角化”的实时量子克雷洛夫子空间（近似求能级的数学子空间）算法，在求解复杂体系哈密顿量基态时实现了接近理论极限的最优量子采样复杂度^[5]。相比传统变分量子本征求解（经典优化辅助求基态）算法普遍受困的贫瘠高原（参数优化梯度指数消失）问题，该算法利用时间反演镜像态直接构建投影子空间，彻底消除了非凸经典参数优化循环，将测量采样次数降低至物理理论下限附近^[5]。算法为中等规模硬件计算复杂强关联分子体系扫清了经典优化瓶颈，预计在2年内整合至Qiskit等主流计算开源框架^[5]。

发表于《Quantum》期刊的科研成果推出了名为SamBa-GQW的非变分连续时间量子行走组合优化算法，能够不依赖任何经典优化器直接求解任意高阶二值组合优化问题^[20]。该算法打破了传统近似优

化算法中经典参数循环带来的算力损耗瓶颈，在大规模二值组合优化问题上的解质量与成功率显著超越传统启发式混合方案^[20]。这为金融投资组合配置、电网实时负载调度等高阶NP难问题提供了全新的量子算法求解框架^[20]。

美国能源部普林斯顿等离子体物理实验室开发出高通量分子动力学模拟新方案，大幅加快了用于量子计算和传感器的高性能金刚石自旋缺陷筛选速度^[7]。该方法将以往需要数月的固态色心材料第一性原理计算周期缩短为数天，直接赋能固态量子存储器与高灵敏微观探针的前端材料设计^[7]。

量子公司Bloq Quantum正式推出面向企业级用户的AI Agent Bloq Maya，旨在消除量子算法开发与异构量子云平台执行之间的底层适配断层^[36]。该软件将复杂的量子电路编译、误差缓解参数寻优以及不同硬件后端的底层指令集转换封装为自动化流水线^[36]。公司宣称其旨在简化与加速企业量子计算应用，加速企业端软件生态渗透^[36]。

04 产业

产业与生态



全球加密资产交易与托管机构Coinbase发布技术立场文件，公开敦促比特币核心社区全面启动后量子密码（抗量子攻击的传统密码）转型准备，严防实用化量子计算机问世直接瓦解现有椭圆曲线签名（主流非对称数字签名）安全体系^[31]。【商业与安全含义】文件强调防护不能仅局限于替换数字签名算法，必须在保证全球节点网络验证效率与区块存储容量的前提下推进向后兼容的协议硬分叉改造；这是全球万亿美元级去中心化金融网络首次由核心龙头出面正式拉响防量子预警^[31]。比特币及整个区块链生态面临底层密码体系洗牌，将倒逼后量子密码迁移从银行、政府外溢至加密金融基础设施，后量子算法审计与节点升级服务将在未来3年催生数十亿美元的市场空间^[31]。

继前期实验室验证后，英国创新署（Innovate UK）正式向Infleqtion英国公司拨付900万英镑（约合1200万美元），专项用于将量子射频（原子能级探测微波信号）测向系统从实验平台推向实际运行环境^{[3][33]}。【商业与技术含义】增量信息显示，该资助标志着基于里德伯原子的高灵敏度电磁信号探测跨过了原理验证期，利用原子内在能级不变性实现全频段、超高灵敏度且抗强电磁干扰的便携化测向装备开发^{[3][33]}。中性原子技术在此展现了在通用容错机成熟前，依托高端国防传感实现早期商业自我造血的落地路径，将巩固Infleqtion在欧美防务采购供应链中的溢价能力^{[3][33]}。

美国本土首座商用量子晶圆代工厂SkyWater Technology与量子退火及门模型双平台上市公司D-Wave签署多年期芯片制造协议，延长并深化双方的代工伙伴关系^[35]。【商业含义】该长约为D-

Wave锁定了全美本土合规的先进超导微纳制造产能，全面保障其特种半导体制造，避免供应链受制于外部封锁^[35]。此合作印证了量子半导体领域“芯片设计与晶圆代工”垂直分工模式的成熟，强化了美国本土超导量子硬件产业链的自主闭环^[35]。

英国科学、创新与技术部宣布启动多项专项资金扶持计划，支持量子初创企业将重力仪、时钟及通信硬件应用于保障铁路准点运行、缩短医院眼底扫描筛查等待期以及军用抗干扰通信^[32]。英国政府从公共财政直接注资基础设施落地，加速量子传感技术在交通、医疗与国防传统产业的快速转化^[32]。

欧洲超导整机企业IQM与澳大利亚斯威本科技大学达成战略合作，建立跨欧洲与亚太地区的量子人才联合培养机制并协同开发工业级应用^[18]。IQM借此将商业触角延伸至印太核心科研圈，通过产学研深度绑定锁定未来区域算力采购客户^[18]。

荷兰量子安全企业QuDef与新加坡创新机构The Thought Projects签署合作备忘录，携手在亚太地区推广量子密钥分发攻防评估与通信物理层漏洞检测平台^[38]。合作填补了亚太地区量子安全硬件物理层测试标准的空白，加速区域内金融与政务通信防护基础设施落地^[38]。

量子安全网络方案商Quantum XChange首席执行官Eddy Zervigon获邀在2026年ACT-IAC网络峰会上主持后量子密码迁移圆桌论坛，针对政企网络防护痛点展开行业研讨^[34]。这反映出美国联邦机构与大型企业对后量子密码替代的关注焦点已从合规讨论转向全网实际部署^[34]。

学术前沿



网络安全机构Certes发表专题评述，针对业界关于“Q-Day”（量子计算机破解主流公钥体系之日）的认知误区提出修正：量子安全威胁的时间窗口并非取决于通用量子计算机彻底建成的时刻，而是取决于黑客当下大规模实施的“先窃听后解密”数据收割行为^[4]。对于国防机密、医疗健康档案及核心金融账本等法定保密期超过10年的高价值资产，现行非对称加密实际上已经失效；网络安全主管必须在当期预算中立刻引入抗量子混编算法与动态密钥体系^[4]。

牛津量子设计公司（Quantum Design Oxford）宣布，德国马克斯·普朗克物质结构与动力学研究所的郭春雨博士荣获2026年度尼古拉斯·库尔特科学奖，以表彰其在理解笼目金属（kagome metals）量子行为方面的基础性发现^[37]。笼目晶格体系中强关联拓扑物态的机理阐明，为设计新一代耐高温、低耗散超导量子芯片提供了重要的凝聚态物理实验支撑^[37]。

06 影响

Downloaded from <http://ajph.org/> at University of California, San Diego on June 11, 2015



万亿加密资产与金融安全体系：受影响方包括全球加密货币持有者、公链核心开发者以及数字资产托管金融机构^[31]。实质改变在于比特币防量子攻击的讨论从极客学术猜想升级为主流机构的技术战略议程，椭圆曲线签名（ECDSA）的替换被摆上桌面^[31]。下一步重点关注比特币核心代码库（Bitcoin Core）是否会提出首个集成后量子

子签名的改进提案（BIP）以及链上硬分叉升级的社区共识演进^[31]。

2 **模块化量子算力预期与二级市场资本**：受影响方包括押注分布式离子阱架构的科技投资人与企业架构师^[11]。实质改变在于第三方对IonQ钇离子-金刚石互连实验的深度拆解暴露了关键指标短板——88%保真度与1千赫兹速率距容错纠错网络门槛存在10至100倍工程鸿沟，打破了短期拼接万比特分布式算力的过度乐观预期^[11]。下一步重点盯紧IonQ是否能在后续预印本中展示纠缠纯化协议实测结果及模块间双比特门的真实保真度分布^[11]。

3 **量子硬件自主代工与半导体供应链**：受影响方包括超导量子芯片设计公司 & 定制晶圆代工厂^[35]。实质改变在于SkyWater与D-Wave签订多年制造长约，确立了超导退火及门模型芯片摆脱科研实验室自建产线、转向标准化商业代工晶圆厂（Foundry）的成熟商业路径^[35]。下一步紧盯SkyWater在全晶圆范围内对超导结电容一致性、超导临界电流均匀度的良率测试报告^[35]。

4 **国防电磁战与野外机动量子传感**：受影响方包括军工电子对抗承包商与前线通信装备部门^[3]^[33]。实质改变在于英国创新署900万英镑拨款推动中性原子里德伯射频测向系统脱离实验室严苛环境，进入车载高机动实战部署阶段^[3]^[33]。下一步关注该系统在野外车载颠簸、宽温区与强电磁压制实战演练环境下的动态测向精度衰减数据^[3]^[33]。

编辑点评

今日的产业与学术动态呈现出清晰的“脱虚向实”分化格局：在通用计算硬件端，早期的公关光环正在被硬核的物理指标核查撕开缝隙。从离子阱模块化光子互连速率与纠错阈值之间10至100倍的理论差距，到超导百比特芯片上“动力学抑制非纠错”的理性澄清，行业正深刻认识到跨越容错门槛绝无捷径，材料层面的微观缺陷与极端光学工程必须逐一攻克。

与硬件端的冷静沉淀形成鲜明对比的是，应用与安全端的防御工程正在全面提速。无论是欧洲航天局跨过1吉赫兹门槛的空间纠缠光子源，还是全球最大加密资产托管机构敲响的比特币换锁警钟，都昭示着量子计算的潜在威胁早已溢出物理实验室，直接扣动了现实金融与数字基建的防御扳机。量子技术对商业世界的重构，注定是防御基建的全面抢跑先于通用算力落地的漫长演进。

参考资料

[1] Powering Energy Solutions: Takeaways from a CCC Community Chat	[4] Q-Day is bad actors monetizing what they' re stealing today.
[2] SQMS Study Links Qubit Performance to Material and Fabrication Features	[5] Mirror subspace diagonalization: a real-time quantum Krylov algorithm with near-optimal sampling cost
[3] Inflection UK to Develop Deployable Quantum Radio Frequency Direction Finding System	

- [6] 'Carpet' growth method yields long-sought 2D quantum material
- [7] Faster molecular simulations identify promising diamond defects for quantum computers and sensors
- [8] New topological microscope tip reveals evidence of 2D altermagnetism
- [9] Quantum physicists trace a century of controlling spin
- [10] Gluon string breaking is simulated using trapped ions
- [11] IonQ Entangles a Trapped Ion With a Diamond Memory 1,000 Times a Second at 88% Fidelity. Its Own Paper Puts the Rate Needed Between Modules 10 to 100 Times Higher.
- [12] IBM and Rutgers Controlled Quantum Chaos on 100 Qubits With Thousands of Mid-Circuit Resets. The Experiment Was Not Quantum Error Correction.
- [13] IonQ Is Buying Elisity for Access to CISOs. Most of the Post-Quantum Capabilities Those CISOs Need First Are Still Missing.
- [14] Postdoctoral Fellowship Position in Rydberg Optical Tweezer Arrays
- [15] Quantum Computing: Tenure-Track Assistant Professor in Computer Science at the University of New Mexico
- [16] Experimental Researcher in Diamond Quantum Science
- [17] Theory of hybrid quantum systems
- [18] Research Engineer in Quantum Computing for Finance - EDHEC Quantum Institute M/F (Postdoctoral Level)
- [19] Swinburne University and IQM Partner to Advance Quantum Ecosystem in Australia and Europe
- [20] Quantum Walks on Arbitrary Spatial Networks with Rydberg Atoms
- [21] Sampled-Based Guided Quantum Walk: Non-variational quantum algorithm for combinatorial optimization
- [22] European Space Agency target met, a gigahertz of entangled photons
- [23] A quantum setup moves from Delft to Karlsruhe
- [24] Scientists recreate a bizarre quantum effect that stops a particle cold
- [25] Hurricane Isaias shows 'it only takes one' to wreak havoc after historically calm Atlantic hurricane season
- [26] Latest Trump administration proposal to change NIH research grant system draws scientists' ire
- [27] The mathematical secret behind why rose petals curl

- [28] OpenAI' s blockbuster Navier-Stokes proof isn' t what we thought it was
- [29] What happens to the body during menopause? New research hints at a biological 'cliff'
- [30] Scientists worry AI is stealing their ideas
- [31] Sex-changing mouse clones may help fight to save endangered species
- [32] Podcasts about the Topic
- [33] Coinbase Urges Early Work on Bitcoin' s Post-Quantum Transition
- [34] Quantum Firms Backed to Keep UK Railways Running And Cut Waiting Lists
- [35] Infleqtion Receives £9 Million to Develop Quantum RF Sensing System
- [36] Google Researchers Propose Using Error Records to Improve Quantum Results After Computation
- [37] Quantum XChange CEO to Lead Post-Quantum Cryptography Panel at ACT-IAC 2026 Cyber Summit
- [38] SkyWater and D-Wave Sign Multi-Year Quantum Manufacturing Agreement
- [39] Swinburne and IQM Partner on Quantum Research and Workforce Development
- [40] Bloq Quantum Launches Bloq Maya AI Agent for Enterprise Quantum Computing
- [41] Quantum Design Oxford Announces Winner of the 2026 Nicholas Kurti Science Prize
- [42] QuDef And The Thought Projects Partner to Bring Quantum Security Platform to Asia-Pacific

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。