

量子计算机破解区块链密钥，门槛更低了

45 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	45
信息来源	9
阅读时长	约 9 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 →](#)

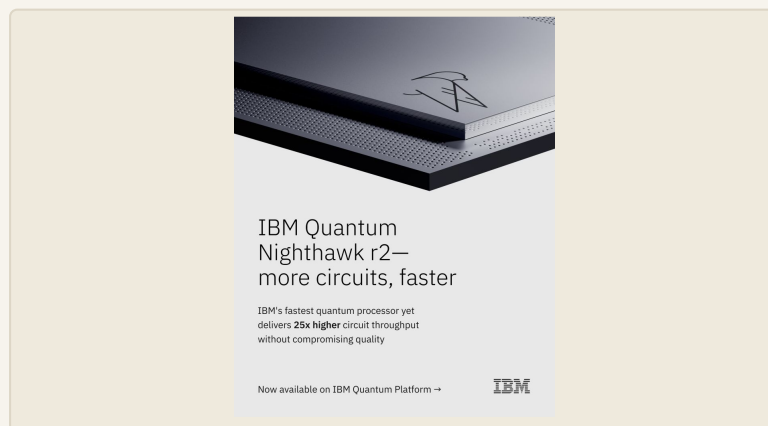
01 亮点

今日三件事



- 量子破解区块链密钥所需资源锐减** 新研究显示量子计算机破解RSA与椭圆曲线密码所需资源更少，威胁比特币等区块链安全^[11]——加密迁移时间表或需提前。
- QTREX Quantum获数千万美元国防大单** 以色列三大防务公司之一部署其AME技术，合同价值数千万美元^[16]——量子技术公司拿到国防级订单。
- Pasqal与True Nexus用中性原子量子技术模拟蛋白质凝胶化** 编码蛋白质结构，模拟液体转凝胶过程^[15]——量子计算切入生物材料研发。

硬件前沿



超导量子处理器

IBM发布Nighthawk r2 QPU（部署为ibm_phoenix），120量子比特，引入高速耗散量子比特复位框架，最大电路吞吐量超过100,000电路/秒，较前代提升25倍^[5]。这是IBM量子处理器中电路吞吐量最高的一次，通过消除电路间空闲期实现。该处理器面向需要大量电路执行的变分算法与错误缓解工作流，用户可更快运行混合量子-经典循环。

硅自旋量子比特

法国Quobly与荷兰TNO及OrangeQS签署两项战略合作协议，推进硅自旋量子比特制造工业化^[4]。协议在法国总统马克龙与荷兰首相耶滕正式国事访问期间签署，两家合作方分别为荷兰应用科学研究组织与自动化测试设备商。Quobly未披露具体保真度指标，但工业化合作瞄准量产一致性。

光子量子硬件

光子量子计算企业Quandela与CMC Microsystems签署谅解备忘录，作为云端量子计算资源提供方加入加拿大的量子计算沙盒^[33]。Quandela未披露平台性能参数，但其加入沙盒将扩大光子路线在北美产业验证中的曝光。

量子退火硬件

超导量子退火器确定了具有长程相互作用的Ising模型基态^[10]。该工作展示了量子退火在复杂磁性晶格模拟中的可行性，但未提供具体退火时间或成功率数据。相比门模型量子计算，退火器在特定优化问题上仍具实用性，但通用性受限。

03 算法

算法与软件



量子算法

PsiQuantum与布鲁克海文国家实验室合作开发容错量子算法，利用Construct平台设计科学应用^[7]。根据协议，布鲁克海文的科学家将使用PsiQuantum

开放访问的Construct软件平台，设计并优化效用级量子工作负载的资源需求。容错算法目前受限于逻辑比特数与错误率，PsiQuantum尚未公开逻辑比特演示。

纠错码

研究人员利用非阿贝尔表面码，在 $D(4N)$ 群的量子双重模型中编码量子比特，实现拓扑保护相位门，且每条边所需量子比特更少^[21]。相比传统表面码，该方案降低了编码开销，但实现需要非阿贝尔任意子，实验难度极高。该工作为拓扑量子计算提供了新的编码思路，但距离物理实现仍远。

量子机器学习

Qilimanjaro训练出99.9%准确率的机器学习读出方案，但该方案并非量子系统，而是用于量子储备计算（QRC）的经典读出层^[9]。QRC仅训练线性读出层，量子系统作为随机非线性映射。该结果表明经典读出层在QRC中可达到高精度，但量子部分是否提供优势仍需验证。

量子模拟

研究人员提出减少多维Caldeira-Leggett模型时空维度的算法，用于高效模拟开放量子系统动力学^[22]。该算法结合降维技术，可降低模拟资源需求，但未提供具体加速比。

量子核物理模拟

两项工作分别利用一阶量子化方法和更少量子比特模拟核动力学^{[19][23]}。其中^[19]使用完整LO阶无介子有效场论哈密顿量，在更少量子比特上取得改进结果；^[23]研究一阶量子化下的实时动力学。相比此前核物理量子模拟，资源需求降低，但距离实际核物理计算仍有差距。

量子蛋白质折叠

Python包QuPepFold实现混合量子-经典蛋白质折叠模拟，CVaR优化VQE达到基态的速度比标准VQE快约30%^[17]。测试对象为最长10个氨基酸的肽段，聚焦内在无序区域。该加速对药物研发早期筛选有潜在价值，但当前规模远小于实际蛋白质。

04 产业

产业与生态



融资与投资

IBM Ventures投资BQP，后者专注于量子算法物理加速，已进入生产阶段^[34]。该轮金额未单独披

露，投资后BQP总融资额达到800万美元，IBM Ventures的入局表明量子算法公司开始吸引产业资本。BQP声称其加速方案已用于生产环境，但未公开性能数据。

国防订单

QTREX Quantum与以色列三大防务公司之一达成数千万美元交易，部署其AME技术^[16]。这是继前几日报道后的新进展：合同金额首次披露为数千万美元。AME技术可能用于量子传感或导航，国防订单将加速该技术的成熟与出口。

政府与政策

塞浦路斯与希腊建立量子安全卫星链路^[35]。该链路由Sparkle与卫星运营商Hellas Sat宣布，旨在保护通信免受未来威胁，是两国之间首条此类连接。量子密钥分发卫星链路目前仍受距离与天气限制，但政府级应用将推动标准化。

合作与生态

QuNorth完成MAGNE量子计算机设施里程碑^[36]。Ramboll已建成容纳MAGNE的专用设施，QuNorth可据此在哥本哈根启动该系统的安装，但未披露具体比特数与性能指标。

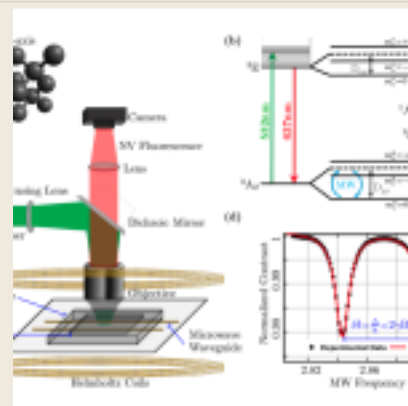
沙特KACST与帝国理工学院合作开展量子大脑研究^[37]。合作聚焦量子计算在神经科学中的应用，可能涉及量子模拟或量子机器学习，但未披露具体项目细节。

企业采用指南

Doug Finke提出四步流程帮助企业用户评估量子技术 [8]。该文面向大型企业管理者，来源摘要未展开四步流程的具体内容，也未包含具体案例或数据。

05 学术

学术前沿



量子信息理论

瑞典乌普萨拉大学招聘量子信息理论方向物理学助理教授，截止日期2026年10月5日 [3]。该职位反映量子信息理论人才需求增长，但未涉及具体研究内容。

量子模拟

康奈尔团队实现光诱导纳米尺度磁化，绕过传统磁体 [12]。该路径可能为自旋电子学与量子存储提供新途径，但未披露具体参数。

量子引力

包括罗杰·彭罗斯在内的国际团队演示下落原子中引力对量子物体的影响^[13]。实验验证了爱因斯坦理论与量子行为的相容性，但未提供具体数据。

量子光学

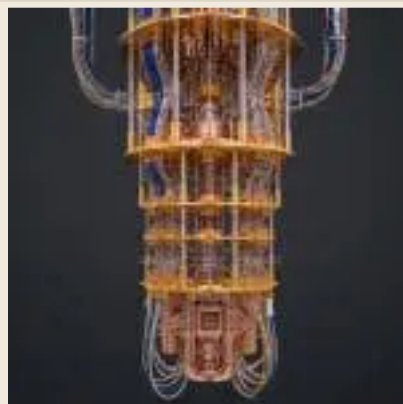
研究人员通过激光整形控制薛定谔猫态几何^[14]。该工作在高次谐波产生中量化相互作用，实现对量子态性质的操控，但未披露具体保真度。

暗物质探测

LZ实验观测到迄今为止最强暗物质信号，可能来自弱相互作用大质量粒子^[18]。LZ实验装置位于南达科他州地下近一英里处，该信号尚未达到发现阈值，需进一步验证。

06 影响

今日影响



- 1 **区块链安全团队：**量子破解资源减少意味着比特币等加密货币的量子威胁时间表可能提前，安全

团队需重新评估迁移至后量子密码的紧迫性 [11]。

- 2 **国防承包商**：QTREX Quantum的数千万美元合同显示量子技术公司已拿到国防级订单，可能引发更多国防订单与出口管制讨论 [16]。
- 3 **药物研发企业**：Pasqal与True Nexus的蛋白质凝胶化模拟若成功，将开辟量子计算在生物材料领域的新应用，药企可关注后续验证 [15]。
- 4 **量子计算云用户**：IBM Nighthawk r2的25倍电路吞吐量提升将加速变分算法开发，用户可更快迭代 [5]。
- 5 **欧洲量子产业**：塞浦路斯-希腊量子卫星链路与Quobly-TNO合作表明欧洲在量子安全与制造自主性上加码，可能影响全球供应链 [35] [4]。

07 编辑

编辑点评

今日量子领域呈现两条主线：一是量子计算对现有密码体系的威胁从理论走向资源估算，二是量子技术从实验室向国防与产业部署加速。前者提醒我们，后量子迁移不再是远期议题，而是需要纳入当前安全规划。后者则显示，量子传感与量子计算正在特定场景中找到付费客户，尽管通用容错量子计算仍有距离。

值得注意的是，硬件进展中IBM的吞吐量提升与Quobly的工业化合作都聚焦于“可用性”而非单纯比

特数，这反映了行业从追求规模向追求实际工作负载的转变。与此同时，算法与软件层面仍缺乏突破性成果，多数进展属于渐进式优化。未来数月，需关注量子破解资源估算是否引发监管行动，以及国防量子订单是否会扩散至更多国家。

参考资料

[1] Corporate and Government Early Adopters in Quantum Chemicals & Quantum Life Science	[9] Qilimanjaro trains new 99.9% accurate machine learning readout, not quantum system
[2] From MIT to IBM, expediting AI and quantum deployment	[10] Quantum annealer finds ground states of complex magnetic lattices
[3] Assistant Professor in Physics specialising in Quantum Information Theory	[11] Quantum computers need fewer resources to break blockchain keys
[4] Quobly Signs Dual Agreements with TNO and OrangeQS to Industrialize Silicon Spin Qubit Manufacturing	[12] Cornell Team Achieves Quantum Light-to-Lasting Magnetism
[5] IBM Releases Nighthawk r2 QPU Featuring Active Dissipative Qubit Reset and 25x Circuit Throughput	[13] International Team Including Sir Roger Penrose Demonstrates Falling Atoms Show Gravity Works on Quantum Objects
[6] QuSecure Achieves TRL-7 at U.S. Army Project Convergence Capstone 6 for QuProtect R3	[14] Researchers Control Schrödinger Cat State Geometry Via Laser Shaping
[7] PsiQuantum and Brookhaven National Lab Partner to Develop Fault-Tolerant Algorithms on Construct Platform	[15] Pasqal's quantum tech models how proteins turn liquids to gels
[8] A Four Step Process for End Users to Leverage Quantum Technology	[16] QTREX Quantum lands deal worth tens of millions with defense giant
	[17] Python package speeds up quantum protein folding by 30 percent
	[18] Dark matter hunt sees strongest signal yet from LZ experiment

- [19] Quantum simulation of nuclei improves on previous work with fewer qubits
- [20] MIT launches quantum fellowships with Moore Foundation support
- [21] Multiverse Computing's Quasar 438B tops European AI scoring
- [22] Anyon Systems and Matrix Group team up to expand quantum computing access
- [23] D(4N) groups create phase gates with fewer qubits per edge
- [24] Reducing Spatial and Temporal Dimensionality in the Multidimensional Caldeira-Leggett Model
- [25] Quantum Simulation of Nuclear Dynamics in First Quantization
- [26] U.N. admits exceeding Paris Agreement's 1.5-degree-C warming target is 'unavoidable'
- [27] Scientists discover a mysterious wave shaped like a decagon in Saturn's atmosphere
- [28] How the super El Niño could turbocharge warming in the Himalayas
- [29] Top medical leaders urge Americans to get their flu and COVID shots in lieu of CDC vaccine campaign
- [30] GLP-1 weight-loss medication could slow aging and extend lifespan
- [31] The risk of high blood pressure in pregnancy is rising—and the damage can be life-changing
- [32] Why this Canadian island appeared to disappear
- [33] Newly discovered 'demon cave fish' hid out in Alabama military installation for 40 years
- [34] The hackers protecting America's water supply
- [35] Quobly and TNO Partner on Silicon Spin Qubit Development
- [36] Quandela Joins Canada's Quantum Computing Sandbox With Photonic Quantum Platform
- [37] Scientists Observe Einstein's Gravity in The Quantum World
- [38] PsiQuantum and Brookhaven Lab Partner on Fault-Tolerant Quantum Algorithms
- [39] Pasqal and True Nexus Apply Quantum Computing to Protein Gelation
- [40] QuSecure Demonstrates Post-Quantum Security for U.S. Army at Project Convergence
- [41] IBM Ventures Invests in BQP as Quantum-Algorithm Physics Acceleration Reaches Production
- [42] Cyprus and Greece Establish Quantum-Secure Satellite Link
- [43] QuNorth Clears Facility Milestone for MAGNE Quantum Computer
- [44] KACST and Imperial College London Partner on Quantum Brain Research
- [45] Langworthy Introduces American Quantum Competitiveness Act

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。