2026 年 08 月 29 日 - 08 月 30 日 · 日报

比特币量子防盗门，现在能真用了吗

22 篇 · 6 个来源 | PDF | 本期汇总免费阅读

本 期 目 录

收录报道	22
信息来源	6
阅读时长	约 10 分钟

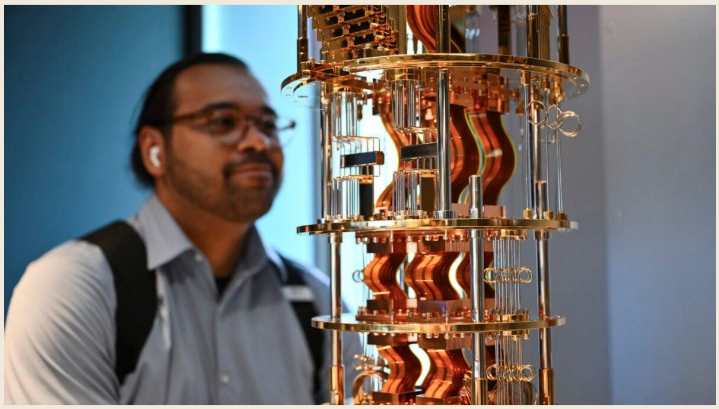
当 前 S O T A

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



1 **量子抗性比特币交易首次上链** StarkWare实验显示比特币用户或许拥有应对量子攻击的应急逃生通道，交易已实际挖出[1]——量子安全从纸面走向链上。

2 **新墨西哥州配套资金押注2033实用量子** 州政府为DARPA量子基准计划C阶段公司提供匹配资金，目标2033年实用规模[13]——政府资金加码量子竞赛。

3 **QuantrolOx与QURECA联手培养量子硬件工程师** 推出Quantum EDGE Academy，用飞行模拟器式软件环境培训自动化QPU操作[4]——量子劳动力缺口获商业化填补。

02 硬件

硬件前沿

量子密钥分发

以15%的量子比特概率检测窃听 实验量子密钥分发在15%的共享量子比特上检测窃听，且不丢弃任何密钥材料；传统方法需揭示并损失密钥比特来验证安全[5]。这是QKD安全验证的新方向，将密码操作嵌入光子量子开关，通过控制量子比特实现隐蔽窃听检测。对QKD实用化影响直接：密钥率损失从传统方案的显著比例降至零，若独立验证成立，将改变QKD系统的安全边际设计。

光子形状编码让密钥率升至0.9 Kb/s 新QKD协议利用光子空间模式编码数据，密钥率达0.9 Kb/s[18]。这属于QKD编码维度扩展，相比传统偏振或相位编码增加了一个自由度。对量子安全网络部署者而言，0.9 Kb/s仍远低于经典通信，但已进入低速物联网等场景可接受范围。

超导量子比特

NIST与马里兰大学提出量子自治门实验方案 研究人员提出实验实现量子自治门，成果于2026年8月28日发表在《Quantum Science and Technology》[6]。自治门无需外部经典控制即可执行量子操作，是减少控制电子学开销的路径之一。对超导路线扩展性有潜在价值，但尚处实验方案阶段，未给出保真度数据，无法对标当前超导双比特门SOTA（99.5%–99.9%）。

离子阱量子比特

几何相位门将纠缠保真度推至0.99以上 研究人员在囚禁离子量子比特上实现贝尔态保真度超过0.99，即使存在多达10个声子的运动激发[10]。这一结果追平离子阱路线头部水平（Quantinuum Helios全比特对F2Q 99.921%，IonQ EQC原型单对99.99%），但报道未说明是单对还是全系统指标；若为单对且无并行数据，则仍落后商用全比特对SOTA一个数量级。距离容错仍缺全系统并行门保真度与可扩展架构验证。

自旋量子比特

冻结杂质让自旋量子比特相干时间达0.2秒 核自旋在固体中是量子网络和量子中继器的主要候选，直接全光初始化、相干控制和读出单个核自旋量子比特一直是挑战；通过冻结顺磁杂质，相干时间超过0.2秒，单发读出保真度达91(2)%[16]。对于全光初始化、相干控制与读出的单个核自旋量子比特而言，超过0.2秒的相干时间是显著进展。但读出保真

度91%仍低于容错阈值（通常要求99%以上），且未说明可扩展性；该结果若经独立复现，将显著改善量子中继器可行性。

拓扑与量子材料

PTB与维尔茨堡探索无磁场量子电阻标准 Kajetan Fijalkowski博士与PTB利用量子反常霍尔效应开发新型电阻标准，无需外部磁场实现高精度[12]。这是计量学应用，量子反常霍尔效应提供拓扑保护的量子化电阻。对精密测量和标准制定有长期影响，但商用时间尺度以年计。

---

03 算法

算法与软件

量子计算机在LHCb碰撞中识别粒子径迹 Nikhef Maastricht的研究人员用量子计算机从LHCb碰撞数据中识别粒子径迹，结果与传统方法相当[15]。这是量子计算用于高能物理数据分析的可行性演示，结果与传统方法相当，但未超越经典方法。对粒子物理界和量子算法开发者有信号意义：量子优势尚未出现，但集成路径清晰。

全息框架连接量子信道行为与拓扑 研究人员提出全息框架，将d维量子信道连接到(d+1)维波函数，揭示自发对称性破缺如何源自边界任意子凝聚[17]。这是理论进展，为量子信道分类和拓扑量子计算提供新视角。对量子纠错码设计可能有长远启发，但短期内无工程影响。

量子机器学习加速量子比特调谐 Quantum Machines与Academia Sinica展示，一个双量子比特门手动调谐通常需约15分钟，使用强化学习智能体可在约25秒内完成校准；连接OPX1000控制器与经典GPU加速器通过OPNIC实现实时硬件反馈连续调谐[11]。这是量子控制自动化的实质性进步：调谐时间缩短约36倍。对量子计算硬件运维成本影响直接，尤其对需要频繁校准的中等规模系统。

---

04 产业

产业与生态

QuantrolOx与QURECA推出量子硬件培训学院 量子测量控制软件开发商QuantrolOx（芬兰埃斯波/英国牛津）与量子教育提供商QURECA（英国格拉斯

哥）合作推出Quantum EDGE Academy，集成到QURECA教育目录中，提供飞行模拟器式软件环境，培训实验人员、技术人员和硬件工程师进行自动化QPU开发、调谐与量子比特表征[4]。商业含义：量子劳动力短缺是行业瓶颈，培训产品货币化路径清晰。对量子公司和招聘方，合格操作员供给增加可能降低人力成本。

新墨西哥州配套资金瞄准2033实用量子计算 新墨西哥州技术与创新办公室为参与DARPA量子基准计划C阶段的量子公司提供配套资金，目标2033年实用规模量子计算[13]。继8月27日报道后，新进展是明确了配套资金与DARPA C阶段挂钩。对量子初创公司，州级资金可降低融资压力；对投资者，政府持续投入强化长期预期。

Nancy Grace Roman望远镜发射升空 NASA的Nancy Grace Roman望远镜已发射，将探测暗物质和暗能量、发现系外行星并研究恒星[20]。继8月28日报道后，新进展是发射已完成。这是天体物理任务，非量子计算，但与量子传感和基础物理研究有交叉；对太空科技板块有市场情绪影响。

05 学术

学术前沿

统一三种量子参考系方法 冲绳科学技术大学院大学（OIST）的研究人员统一了三种内部量子参考系方法，推进量子引力、规范理论和基础物理研究[8]。这是理论框架整合，将三种内部量子参考系方法纳入统一描述。对量子引力实验设计有潜在指导意义，但距离实验验证尚远。

超导纳米结中量子干涉导致超流振荡 新理论详细说明安德烈夫态的量子干涉如何影响超导纳米结中的超流，揭示在势垒透射率低于1时出现相干振荡[9]。这是凝聚态物理理论进展，对超导量子器件设计有参考价值。对量子计算硬件，可能改善约瑟夫森结建模，但短期无直接影响。

量子冷却比看上去更难 研究解释，尽管实际系统散热高效，但在量子计算机上采样平衡分布（模拟冷却的关键步骤）仍然困难[14]。这属于量子算法复杂性结果，对量子模拟冷却过程设定了边界。对材料科学和药物设计中的量子模拟应用，提示冷却模拟可能不是近期优势场景。

主动规范场实验实现 伊利诺伊大学与伯明翰大学研究人员实验实现了可调非阿贝尔规范场，利用振荡

器产生局域赝自旋并通过实时反馈工程耦合[7]。这是量子模拟的重要一步，非阿贝尔规范场是粒子物理标准模型的核心结构。对量子模拟器研究高能物理有直接推动，但距离实用化仍有差距。

量子引力迹象或为幻觉 新理论框架表明，一些看似显示引力量子行为的实验可能有更普通的解释；研究人员发现涉及所谓“引力叠加”的场景可以被经典模型复现[19]。这是对量子引力实验证据的挑战，提醒学界谨慎解读。对量子引力研究社区影响显著，可能引发实验设计重新评估。

06 影响

今日影响

1. **比特币持有者获得应急方案**：StarkWare的量子抗性交易已实际挖出，显示比特币或存在应对量子攻击的应急逃生通道[1]；短期关注是否出现类似方案的标准化讨论。

2. **量子硬件运维成本有望下降**：强化学习调谐将双量子比特门校准从15分钟缩至25秒[11]；量子计算公司可减少人工调谐时间，加速设备周转。

3 **量子安全通信研究提速**：15%量子比特窃听检测和光子形状编码QKD[5][18]为QKD实用化提供新路径；电信和金融安全团队应跟踪后续独立验证。

4 **量子劳动力培训商业化启动**：QuantrolOx与QURECA的培训学院[4]填补硬件操作员缺口；量子公司招聘压力可能缓解。

5 **政府资金持续加码量子竞赛**：新墨西哥州配套资金[13]强化美国州级对实用量子计算的支持；投资者可关注获配套资金的初创公司。

07 编辑

编辑点评

今日最值得关注的是量子安全从理论走向链上：比特币量子抗性交易的实际挖出，标志着加密货币社区开始认真对待量子威胁。这并非技术突破，而是工程验证——显示在现有基础设施上尝试增加量子安全层是可行的。对投资者而言，这降低了量子计算机突然威胁比特币的尾部风险，但需注意该方案仍属实验性质，未经过大规模审计。

另一个趋势是量子控制的自动化：从量子自治门到强化学习调谐，减少人工干预正在成为硬件扩展的必经之路。当前量子计算机的运维成本中，人工校准占比可观，自动化工具的商业化将改变量子公司的成本结构。未来一年，我们应关注此类工具是否

被头部硬件厂商集成，以及是否出现独立的校准服务市场。

参考资料

[1] The First Quantum-Resistant Bitcoin Transaction Has Been Mined

[2] 27th Asian Quantum Information Science Conference

[3] RIMS International Symposium "Mathematics of Quantum Information Science"

[4] QuantrolOx and QURECA Partner to Launch Quantum EDGE Academy for Hands-On Hardware Training

[5] Researchers Detect Eavesdropping with 15% Qubit Probability

[6] NIST and University of Maryland detail autonomous quantum control

[7] Canada invests $195M in Xanadu for quantum computer manufacturing

[8] University of Illinois & Birmingham Build Active Gauge Field

[9] Okinawa Institute scientists unify three quantum reference frame methods

[10] Supercurrents oscillate with quantum interference in nanojunctions

[11] Geometric phase gates boost ion qubit entanglement fidelity

[12] Quantum Machines and Academia Sinica speed up qubit tuning with AI

[13] PTB & Würzburg Explore Quantum Magnet-Free Resistance Standard

[14] New Mexico funds target utility-scale quantum by 2033

[15] Cooling quantum systems is harder than it looks, study explains

[16] A quantum computer spotted particle paths in LHCb collisions

[17] Freezing impurities extends spin qubit coherence to 0.2 seconds

[18] A holographic framework links quantum channel behavior to topology

[19] Encoding data in photon shape boosts quantum key rates to 0.9 Kb/s

[20] Some signs of quantum gravity may be an illusion

[21] NASA’s Nancy Grace Roman Telescope launches to space

[22] Why obsessing over self-improvement could be sabotaging your brain

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。