標題：量子技術突破 **ECC** 加密防線：全球加密基礎設施的危機與 **PQC** 轉型對策

這一切正在發生！

📘 Google 量子 AI 團隊剛剛完成了一項創舉：他們成功對比特幣與以太坊所使用的 ECC 橢圓曲線加密演算法，進行了實質且可驗證的破解。他們利用 50 萬個超導量子位元 (superconducting qubits)，在短短約 9 分鐘內就完成了這項任務。這不是紙上談兵的理論，而是已經透過零知識證明 (zero-knowledge proof) 確認的現實。

📗 與此同時，Oratomic（與加州理工學院及加州大學柏克萊分校合作）也達成了相同的破解結果。他們使用的是中性原子 (neutral-atom) 系統，僅僅用了 1 萬個量子位元。雖然運算時間花了幾天而非短短幾分鐘，但所需的量子位元數量卻足足少了 50 倍。

📊 兩種截然不同的量子架構，卻指向同一個明確的威脅。

📉 真正的危險並不在於單一技術的突破，而是這些技術的「收斂」。目前橫跨超導與中性原子平台的四項獨立研究（Gidney 2025、Pinnacle 2026、Google 2026、Oratomic 2026），都不約而同地將破解門檻縮小到同一個區間：1 萬到 100 萬個量子位元。

🔐 在每一種經過測試的架構中，保護著幾乎所有加密貨幣錢包的 ECC 防線，都比傳統的 RSA 更早崩潰。Google 針對 ECC-256 的攻擊，所需的量子位元數量大約只有 Gidney 預估破解 RSA-2048 的一半。而 Oratomic 的中性原子系統破解 ECC 只需要 1 萬個量子位元，相較之下，破解 RSA 則需要 10.2 萬個。

一台擁有 1 萬個量子位元的中性原子電腦，也許還無法即時攔截你的下一筆鏈上交易；但它絕對有能力「回溯」並掏空數百萬個休眠錢包——那些公鑰早已暴露在區塊鏈上，且資金一直沒有移動的錢包。

🛡️ 好消息是：美國國家標準暨技術研究院 (NIST) 的後量子密碼標準（ML-KEM 與 ML-DSA）已經定案，並隨時可以投入部署。轉型的路徑已經明確。

更好的是，G7 已經公開分享了 PQC (抗量子密碼) 的遷移藍圖，為各國政府、企業及開發者提供了一個全球協調的時間表與技術指南。https://lnkd.in/eM3cFepc

然而，挑戰依舊嚴峻：機構級的密碼系統轉型通常需要花上數年的時間，但現在量子硬體的發展速度，已經是「以年為單位」，而非過去所以為的「以十年為單位」了。

所謂的 Q-Day（量子運算攻破現有加密技術之日）並不會在明天就到來。但是，「完成轉型實際所需的時間」與「新硬體問世的速度」之間的緩衝期，已經被急遽壓縮。

是時候採取行動了。

#pqc #後量子密碼學 #nist #g7 #pqc轉型