量子计算会威胁比特币安全吗？（下）
——谷歌白皮书对增强网络安全有何现实意义？

文丨徐令予

谷歌这份白皮书的内容大致可以归纳为三个方面：其一，对破解现有密码体系所需的量子计算资源给出了新的估算；其二，引入零知识证明，对这些估算结果进行了验证；其三，在此基础上，讨论了与密码相关的量子计算机（CRQC）对加密货币安全的影响，并提出了应对策略。

此前，我们已通过两篇文章解读了白皮书“披露了什么”与“验证了什么”。本文将把目光锁定在最后一环：面对 CRQC 的威胁，谷歌究竟提出了哪些御敌之策？这些方案对加密货币的底层安全又有什么现实意义？

谷歌的白皮书并不是一篇传统意义上的科学论文，而更接近一份面向工程与安全领域的政策文件。它的目标，并不在于提出新的技术并给出严格证明，而在于对潜在风险进行分析，给决策层敲响警钟，促使相关行业提前修筑“防火墙”。

从这个维度观察，谷歌的态度显得相当克制且务实。白皮书虽然指出了量子计算在理论上对公钥密码的安全构成威胁，但并未贩卖焦虑。它反复申明，破解公钥密码的具体时间仍存在不确定性。它拒绝将“实验室里的潜力”与“现实中的战力”画等号，在风险预警与过激反应之间，拿捏住了一种微妙的平衡。

遗憾的是，这种难得的“分寸感”在二次传播中往往被丢弃了。不少媒体在转述时，更热衷添油加酱、捕风捉影，从而营造出一种“大难临头”的错觉。

正因如此，我们更有必要拨开迷雾、看清真相，对量子计算与加密货币安全的博弈做一个清醒的研判：这场威胁究竟走到了哪一步？面对未知的算力怪兽，我们该如何制定一套既现实又明智的安全策略？

一、近忧还是远虑？量子威胁的虚实边界

与密码相关的量子计算机（CRQC）对广泛部署的公钥密码学构成了威胁，其中包括（RSA）密码和椭圆曲线密码（ECDLP）。前者所受威胁源于 Shor 提出的针对整数分解的高效量子算法，后者所受威胁则源于 Shor 提出的针对椭圆曲线离散对数问题的高效量子算法。

在这些易受量子攻击的密码学应用场景中，加密货币因以下两个原因而显得尤为突出。首先，为了追求效率和规模，许多区块链系统对基于 ECDLP 的密码存在高度依赖；在提供同等安全强度的前提下，基于 ECDLP 的密钥长度仅为 RSA 密钥长度的约十分之一。这意味着只需一台规模相对较小的 CRQC 便有可能将其破解。其次，与通常采用多重安全防护机制的传统金融体系不同，区块链系统往往不提供针对欺诈性交易的追索机制；一旦攻击者伪造了某项数字签名，便可实施不可逆转的盗窃行为。

然而，量子攻击真要得手也受到不少条件的制约，它不仅受限于量子资源的规模，更取决于目标系统的安全设置。例如，比特币的“工作量证明”（PoW）共识机制能够免疫基于 Grover 算法的量子攻击；Zcash 最新的“屏蔽池”（shielded pool）能够抵御针对协议参数的量子攻击；此外，包括比特币在内的许多区块链系统中，公钥通常被置于加密哈希函数的保护之下，从而获得了有效的防护。这意味着，风险并非普遍存在，受影响的只是一些特定类型的加密资产。

更为关键的是，从工程角度看，这一威胁仍非燃眉之急。白皮书所给出的资源估算，虽然相比以往有所收紧，但仍然需要上千个逻辑量子比特以及数千万级别的量子门操作。即便不考虑纠错开销，这一规模与当前可提供的量子计算硬件资源之间，仍存在跨数量级的鸿沟。更遑论实际运行中面临的退相干噪声控制与高保真纠错等复杂的工程挑战。

因此，白皮书的意义并不在于展示量子攻击的现实能力，而在于对未来可能性的重新界定。它通过更具体的资源估算，以及相应的验证方法，使原本较为抽象的风险讨论获得了更清晰的量化标准。但这种“更清晰”，并不等同于“更接近”。它缩小的，是理论上的不确定性，而不是现实中的距离。

二、时间是变量，应对是定力

白皮书指出，尽管时间裕度在收窄，但具备实质威胁的量子计算机（CRQC）问世前，我们仍有充足的窗口期完成区块链向后量子密码（PQC）的迁移。

为此，本文更新了量子攻击的资源估算，并深度剖析了安全漏洞与缓解方案，旨在敦促加密社区即刻启动 PQC 迁移——因为在当前技术节点，按时完成迁移仍具高度的可行性。

核心逻辑在于：风险的本质是时间的博弈。在量子算力足以攻破现行体系前，公钥密码仍处于“可控防御期”。

在此窗口期内，采取分阶段应对策略至关重要。

- **短期策略——收缩攻击面**：风险主要集中在公钥已经暴露的资产上，因此通过减少地址复用、缩短公钥暴露时间等措施，可以在一定程度上降低攻击面。这类措施虽然无法改变底层密码机制，但能够显著影响潜在攻击的实际可行性。相较于全面升级底层的密码系统，这些过渡性措施在技术上更为简易，从而能够更早地得到部署与实施。
- **长期策略——系统性升级**：真正的解决路径仍然在于密码算法的升级，即逐步向后量子密码过渡。这一过程并非简单的算法替换，而是涉及协议层升级、系统兼容以及生态协同等一系列问题。正因为这一过程复杂且周期较长，它需要在风险尚未迫近之前就开始规划，而不是在威胁显现之后被动应对。

幸运的是，实现加密货币后量子安全性的路径已清晰可见。后量子密码学（PQC）目前已演进为成熟的学科体系：相关的加密算法方案不仅通过了学术界的严格审查，更已步入标准化的实施与部署阶段，为系统迁移提供了坚实的理论与工程支撑。

综上所述，这份白皮书的核心价值，在于为量子计算与加密货币的博弈给出了基于实证的理性研判：

理论维度： 威胁确实存在，不可视而不见；
工程维度： 距离实战尚远，无需过度恐慌；
实践维度： 应对方案明确，尚有时间窗口。