quantus

量子安全，加密货币

发布	版本	分类
2026年3月21日	0.3.3	public

本白皮书仅供信息参考， 不构成出售要约、购买要约招揽， 或对任何证券、投资或金融产品的推荐。读者在做出投资决策前应自行尽职调查， 并咨询合格专业人士。 Quantus Network 不对本文所含信息的准确性或完整性作出任何陈述或保证。

目录

01

引言

量子威胁

传统区块链面临来自 密码学相关量子计算机（CRQC）的生存威胁。区块链的 密码学基础依赖于 离散对数问题（DLP）的难度，而量子算法， 尤其是 Shor 算法，可以以指数级快于 经典计算机的速度求解 DLP。这一漏洞可能使量子 对手从公钥推导出私钥，从而 伪造交易并解密敏感的金融 数据。

> 若无主动的抗量子升级，数万亿美元的加密经济 可能因此类攻击而突然贬值。

独特价值主张

Quantus Network 以拉丁语中表示「多少」的词命名， 提供可扩展、量子安全的隐私货币。Quantus 不是通用 智能合约平台。如同一家只提供少数几道 精心打磨菜品的餐厅，Quantus 提供：

- 所有交易均采用后量子签名
- 后量子签名与加密（ML-DSA 与 ML-KEM）保护对等节点连接
- 后量子零知识证明以实现扩展
- 高安全性账户以遏制盗窃并支持从错误中恢复
- 可读校验短语，便于简单验证地址

聚焦可扩展、量子安全的隐私货币这一决策， 源于 CRQC 对行业的威胁，以及比特币 无力应对这些挑战。

02

区块链面临的量子威胁

量子计算基础

量子计算机利用叠加与 纠缠等原理，执行对 经典机器而言难以处理的计算。与只能为 0 或 1 的经典比特不同， 量子比特（qubits）可同时处于多种状态， 为特定问题带来指数级并行。这一 能力对支撑区块链金融的密码系统构成生存风险，因为为 量子硬件开发的算法动摇了大多数 公钥密码学的安全假设。

Shor 算法由 Peter Shor 于 1994 年提出，在量子计算机上为分解大整数和求解 离散对数问题提供 多项式时间方法。它利用量子 傅里叶变换（QFT）寻找函数的周期， 从而高效逆转支撑 RSA 或椭圆曲线密码（ECC）等方案的陷门函数。对区块链 金融而言，这意味着拥有足够强大的量子计算机（估计约 2,000 个逻辑量子比特 [6][7][8][9]） 的攻击者可在多项式时间 $O(n^3)$ 内从公钥推导私钥：极端的加速 使脆弱系统一夜之间过时。 [1]

Grover 算法由 Lov Grover 于 1996 年提出，为非结构化搜索提供 平方加速，将搜索时间从 O(n) 降至 $O(\sqrt{n})$ 次操作。虽不如 Shor 对非对称密码那样致命，Grover 仍影响哈希函数与 AES 加密等对称原语，实质上使安全级别减半（例如 256 位密钥 在量子攻击下表现得像 128 位）。该攻击通过 将安全位数加倍而非更换 密码方案来缓解。此外，Grover 的平方加速因极高的量子比特与门需求而在实践中难以落

地， 需要数十亿次顺序操作且并行度有限， 即便在未来硬件上，对现实世界的逆向仍不经济。[2]

四类威胁

01 - 伪造数字签名

Shor 算法直接威胁大多数区块链使用的基于 ECC 的签名 （例如比特币的 secp256k1 曲线），使 对手可冒充用户并授权欺诈 交易。这种能力将构成区块链 最基本功能的灾难性失效。

02 - 在零知识系统中伪造无效证明

许多零知识证明，例如面向隐私金融的 zk-SNARKs， 依赖椭圆曲线配对实现的离散对数难度来承诺。Shor 可能允许 创建看似有效实则无效的证明，使攻击者可铸造新币或伪造 Layer 2（L2）状态。

03 - 解密秘密信息

量子攻击可能暴露 Zcash 或 Monero 等隐私协议中受脆弱公钥方案保护的加密数据；也可能解密金融协议中的 p2p 通信， 泄露敏感财富细节并促成定向盗窃。

04 - 逆向哈希函数

Grover 算法可加速对 SHA-256 等哈希的原像攻击（用于工作量证明与地址生成），但 这是最不令人担忧的威胁。许多后量子 密码方案采用基于哈希的构造，因为只要摘要足够大， 哈希仍被认为足够安全。

后量子密码中的扩展挑战

尽管后量子密码（PQC）为抵御 量子威胁提供必要保护，但由于这些算法的固有设计， 会引入显著的扩展障碍。 与依赖紧凑数学结构的椭圆曲线方案不同， PQC 原语需要更大参数以维持对经典与量子 对手的安全性。这导致公钥、私钥与签名明显更大， 往往相差数个数量级。下表 展示 128 位后量子安全级别下 ML-DSA 的典型规模， 相对 256 位 ECDSA 等经典等价物：[10]

算法	公钥	私钥	签名
ML-DSA-87 (Dilithium)	2,592 bytes	4,896 bytes	4,627 bytes
ECDSA (256-bit)	32 bytes	32 bytes	65 bytes

128 位后量子安全级别下的规模。来源：Open Quantum Safe Project [10]

可见，ML-DSA 签名可比 ECDSA 等价物大 70 倍以上，公钥大 80 倍以上。 其他 PQC 家族更甚：基于哈希的方案如 SPHINCS+ 可产生高达 41 KB 的签名，而像 FALCON 这类尺寸优化格变体 仍显著大于经典规模。

在区块链语境下，这些膨胀的规模会累积为 系统性扩展问题。更大的签名使单笔交易膨胀，区块更快填满并需要更长验证时间，从而降低每秒交易数（TPS）。同时挤压点对点（P2P）通信，增加带宽与 传播延迟，在工作量证明等共识机制中可能提高分叉或 孤块风险。 存储

需求亦受影响，节点运营成本更高、参与门槛更高，尤其对 资源有限的用户或验证者。

> **说明**
>
> 所有区块链未来都必须应对这些扩展挑战。例如，若不提高最大区块大小， 比特币的 TPS 将远低于 1。

03

迁移危机

协调问题

比特币的保守文化抵制协议变更。任何 PQC 改进 都需在迁移期限、可能的代币没收与区块大小增加等有争议问题上达成共识。 即便社区同意，每位用户 也必须将资金迁移到量子安全的新地址。 迁移要求所有加密资产持有者行动， 其中许多人已丢失钱包访问权限或忽视威胁。

这些问题存在于所有公链，但对比特币尤为 困难，因其缺乏明确领导且奉行 技术僵化哲学。

丢失币问题

据估计约有 2500 亿至 5000 亿美元的比特币因密钥丢失、持有人去世或 遗忘钱包而永久无法访问。[3] 这些币无法迁移，相当于公开悬赏制造密码学相关量子计算机（CRQC）。量子攻击者将从未迁移的公钥推导私钥，并可能将数百亿美元 的 BTC 倾泻到市场。

> 唯一的技术方案需要严格的期限 冻结未迁移的币：这在政治上 不可行。

若无此类期限，未迁移的币将被盗取并出售，冲击市场并摧毁 对网络的信任。

迁移时间表问题

后量子签名比当前比特币签名大约 20 至 80 倍。 若无根本性架构变更，比特币性能 将跌至本已有限的容量的一小部分。

假设比特币解决政治与技术挑战， 迁移本身仍需数月或数年。每位持有人至少需 发送一笔交易，将资金移至量子安全地址。 许多人会先发送试探交易。臃肿的 PQC 签名压制吞吐时，网络将面临持续数月或数年的队列，而量子脆弱资金仍暴露在外。

> **QUANTUS 的回应**
>
> 这些叠加的挑战使向现有链添加量子安全变得极其困难。Quantus Network 通过从第一天起将量子安全内置于链上来规避这一问题。

04

quantus network 架构

基础

Quantus Network 构建于 Substrate 之上，这是由曾参与 Ethereum 与 Polkadot 的 Parity Technologies 开发的区块链 SDK。Substrate 高度模块化，便于替换组件以聚焦 Quantus 的独特之处。

Quantus 对 Substrate 的增强包括：

- 增加后量子签名方案支持
- 将网络 p2p 安全升级为后量子
- 增加用户可控的交易可逆性
- 通过将所有数据类型与域元素边界对齐，使数据库与 zk 兼容

后量子密码原语

Quantus Network 采用 NIST 标准化的 PQC，确保交易与网络通信在量子威胁下的安全。交易完整性的核心是 **ML-DSA** （基于模格的数字签名算法，曾名 CRYSTALS-Dilithium），一种基于格的签名方案，因其在安全性、效率与实现便利性之间的平衡而被选中。ML-DSA 利用 Learning With Errors（LWE）与 Short Integer Solution（SIS）在 模格上的难度等问题，对包括 Shor 算法在内的经典与量子攻击提供强韧抵抗。[4]

对交易签名，Quantus 集成 **ML-DSA-87**，即最高安全级别参数集（NIST 第 5 级， 相当于经典 256 位与量子 128 位）， 以防范格密码分析的可能进展。该选择侧重审慎，因格密码相对新颖，实战检验少于经典方案。 更大参数可缓解格密码分析潜在突破的风险，较小密钥尺寸反而可能成为更弱目标。

备选方案

相对 FN-DSA（Falcon）等替代方案选择 ML-DSA，因 FN-DSA 实现更复杂（例如需要 浮点运算，不适合区块链）、规范中无确定性密钥生成，且开发时尚未最终定稿。

未选择基于哈希的 SLH-DSA 等选项，因其签名更大（超过 17 KB）。密码敏捷性 （可更换签名方案）已内置于 Substrate，未来若情况需要，添加这些替代相对容易。

尽管 ML-DSA-87 产生更大密钥与签名，在 Quantus 早期网络中仍可管理，此时存储尚非瓶颈，且 wormhole 地址配合 零知识证明等优化将解决扩展问题。

实现技术细节见 QIP-0006。

libp2p — 量子安全的网络

Quantus Network 通过结合 ML-DSA 认证 与 **ML-KEM**（基于模格的密钥封装机制， 曾名 CRYSTALS-Kyber）加密，保护点对点（P2P）节点通信。该集成将 PQC 延伸至 libp2p 栈，修改 核心组件以实现抗量子：ML-DSA-87 签名用于对等身份，ML-KEM-768 用于传输安全

（通过向 Noise 握手增加额外 KEM 消息以获取抗量子共享密钥）。[5]

P2P 层在量子安全分析中常被忽视。 对等认证重要，但攻击者在 P2P 层最坏情况是冒充节点并发送无效 消息，可能导致拒绝服务。该风险已因区块链模型中节点通常不受信任且检测到攻击后可轻易换钥而缓解。同理，解密 P2P 通信对攻击者收益有限（例如追踪交易路径，可用代理或 Tor 缓解），且多数数据最终链上公开。

尽管如此，对 P2P 层做量子安全加固可抵御 窃听、中间人与量子解密， 确保节点 gossip、区块传播及其他网络交互在可预见未来仍保密且完整。

技术细节见 QIP-0004。

pqc 扩展 — wormhole 地址

为应对后量子密码固有的扩展挑战，Quantus Network 引入一种创新的聚合后量子签名方案 **「Wormhole Addresses」**。 该系统利用 Plonky2 证明系统（本质为 STARK）生成的零知识证明（ZKP）， 将余额验证移出链上，使链仅需验证单一紧凑证明而无需处理单笔签名。 Wormhole Addresses 可用一条证明验证大量 交易，主要限制来自公开输入（如 nullifier、 存储根、输出地址与金额）。这使摊销到每笔交易的存储需求降至约每交易额外 256 字节， 远低于任何已知 PQC 签名方案。

该方案的量子安全来自使用抗碰撞哈希函数 **Poseidon2** 通过 FRI（Fast Reed-Solomon Interactive Oracle Proofs）做承诺，而非

SNARK 中常见的易受量子威胁的椭圆曲线配对。

此外，认证秘密隐藏在 Poseidon2 之后。安全哈希仅被 Grover 算法二次削弱， 不会「破解」；哈希原像证明可在 ZK 场景中充当轻量后量子签名， 类似 SPHINCS+ 等基于哈希的方案。

客户端 / 证明者流程

用户生成可证明不可花费的地址，通过对盐与秘密拼接后双重哈希：

```
H(H(salt|secret))
```

该构造避免假阳性（例如将简单哈希公钥与不可花费地址混淆），因为在 Substrate （及一般区块链）中，地址是对公钥的单一哈希，公钥由私钥经某代数运算导出， 而非安全哈希。构造安全性因此归结为寻找安全哈希的「原像的原像」。发往该地址的代币实质被销毁。 无法花费，因接收地址无私钥对应。这些币可重新铸造 而不膨胀总供应。

每笔转账创建存储对象 TransferProof， 包含如全局唯一转账计数等细节。用户钱包从最近区块头的 存储根生成 Merkle-Patricia-Trie （MPT）存储证明至该 TransferProof 的叶子。 计算 nullifier 以防止双花：

```
H(H(salt | secret | global_transfer_count))
```

聚合器流程

任意方（客户端、矿工或第三方）可通过 Plonky2 递归聚合多份 证明，形成证明树，父证明验证子证明并聚合子公开输入：

- nullifier 原样传递
- 输出地址去重
- 区块哈希证明链接后仅保留最新
- 重复输出地址的金额相加

链 / 验证者流程

网络验证聚合证明：区块哈希在链上且为近期、nullifier 唯一（防双花）、证明有效。ZK 电路约束存储证明正确性、 nullifier 精确、地址不可花费、 输入输出余额一致及 区块头链接。

为何选择 plonky2

- 已审计
- 后量子
- 无 trusted setup
- 证明 / 验证高效
- 证明聚合顺畅
- Rust 原生实现
- 兼容 Substrate 的 no-std 环境

> **性能**

> 递归证明在约 170 毫秒内完成，体积紧凑（聚合证明约 100 KB）。在理想情况下，5 MB 区块且所有交易指向同一输出时，Wormhole Addresses 单块可打包约 153,000 笔交易（4.9 MB / 每笔 nullifier 32 字节）：相对约 685 笔原始 ML-DSA 交易（5 MB / 每笔 7.3 KB）约为 223 倍提升。

安全说明

潜在风险包括电路 / 验证实现缺陷导致的通胀错误， 但若重新铸造超过零发送地址余额，经济上可发现。用户可选择发布第一重哈希（不泄露秘密）证明某地址为 wormhole。验证交易无签名，故需以非金融手段缓解失败交易的拒绝服务。代币供应核算仍成立，因重铸表现为新币但通过销毁维持最大供应保证。

更多技术细节见 QIP-0005。

共识机制

Quantus Network 使用工作量证明（PoW）共识算法， 在保留比特币共识理想性质的同时， 通过将 SHA-256 替换为 **Poseidon2** 以更好兼容 ZK 证明系统。

重要：此变更并非出于量子安全。 SHA-256 等密码学哈希被量子算法（尤其 Grover）削弱但未被摧毁。 部分后量子签名方案以安全哈希为基本构件亦出于此因。

Poseidon2 是 Poseidon 哈希的改进。为使用 SHA-256 等传统哈希的计算构建 SNARK 或 STARK 通常需要约多 100 倍的 门，而 Poseidon

完全基于域元素的代数函数而非位运算。

我们对 Poseidon2 与 Plonky2 使用 **Goldilocks 域**。Goldilocks 域阶可容纳于 64 位无符号整数，提高效率而不损害稳健性。

05

财富保全

管理加密货币密钥存在诸多风险，其中大多数 可以避免。

可逆交易

Quantus Network 提供用户可配置的可逆交易。 发送方可设定时间窗口，在此期间可取消对外转账。这有助于遏制盗窃并在不牺牲终局性的前提下纠正错误。系统使用修改过的 Substrate「scheduler」pallet 与时间戳。钱包为发送方显示倒计时（带取消按钮）并为接收方显示。

可逆交易在链上执行的前提下支持新颖安全协议并保持 去中心化。

更多技术细节见 QIP-0009。

校验短语

Quantus Network 引入「check-phrases」，一种可读且密码学安全的区块链地址校验和。对地址哈希生成来自 BIP-39 词表的短词序列。校验短语有助于防范笔误、篡改与地址投毒攻击。50,000 次迭代的密钥派生函数提高彩虹表攻击成本。大额交易用户仍应逐字核对地址。

更多技术细节见 QIP-0008。

高安全性账户

任意账户可升级为「高安全性账户」，对所有对外转账强制可逆期。指定的 **监护人**（硬件钱包、多签或可信第三方）可在可逆期内取消可疑交易，将资金转给监护人而非发送方或接收方。该可选功能一旦启用即永久有效，防止窃贼自行关闭。

监护人可链式配置：高安全性账户的监护人本身可以是带另一监护人的高安全性账户。形成可组合层级，每位监护人对所保护账户拥有更高权限。该设计给用户时间发现与应对未授权活动，而不损害合法转账的终局性。

更多技术细节见 QIP-0011。

密钥恢复

许多加密财富随持有人离世而永久丢失。 Quantus Network 提供简单方式指定可随时提款的恢复地址，但受固定延迟约束。延迟期间，若持有人仍能访问密钥，可拒绝恢复。该功能实现链上「遗嘱」而无需法院或正式继承程序。

hd-lattice

分层确定性（HD）钱包是行业 标准，允许用单一助记词备份所有 密钥，相较每笔操作手动抄写更安全便捷。将其适配 Dilithium 等格方案面临两项 挑战：

— HMAC-SHA512 输出无法直接构成格私钥（格上采样的多项式需满足特定性质）。

— 非硬化密钥派生依赖椭圆曲线加法，格上不存在（公钥对任意代数运算不封闭）。

Quantus Network 对第一点将 HMAC 输出用作熵以确定性构建私钥，而非直接作为密钥本身。第二点重要性较低，格密码能否适配仍是开放研究问题。

更多技术细节见 QIP-0002。

06

代币经济学与治理

Quantus Network 处于变化环境中，无法假设 一次就做对。因此我们选择简单起点，并允许治理系统随新信息演进。该设计使区块链成为可适应环境的活体。尤其 Substrate 的治理流程 可在各节点运营商最小协调下对链进行深度变更。

区块奖励

Quantus Network 采用模仿比特币的简单代币模型。最大供应为 **2,100 万枚**，简单启发式决定每块奖励：

```
block_reward = (max_supply - current_supply) / co
```

该启发式在 `current_supply` 随 `block_reward` 增加时形成平滑下降的指数曲线，从而降低下一区块计算的 `block_reward`。手续费等销毁降低 `current_supply` 并计入区块奖励预算。选择常数使得在无销毁情况下约 30 年可发行 99% 的币。

投资者分配

Quantus Network 在投资者承担高风险资助下建成。私募投资者受 4 年归属期约束， 与团队一致。公募投资者首日即可全额流通。公募所募资金将 与代币配对并用于流动性（DEX、CEX 与做市商）。这些投资者分配与流动性构成唯一「预挖」。其余代币须挖至存在。

若公募售出低于 10% 上限，流动性代币将按比例削减，其余通过区块奖励向矿工发行。

公司分配

为补偿团队承担无成功保证的新技术建设风险，约四年内部分区块奖励流向 公司。这相当于公司总供应约 **15%** 的事实归属期。

此后，公司在区块奖励中的份额可根据代币持有人投票关闭、调整或重定向。

交易手续费

交易类型	手续费结构	去向
标准	固定费用	矿工
可逆（高安全）	按金额 1%	销毁
ZK 聚合	按金额 0.1%	50% 矿工 / 50% 销毁

无分叉升级

Quantus Network 通过 Substrate 的 runtime 升级支持「无分叉」升级，使区块链核心逻辑（「runtime」）演进而无需扰乱网络或分裂社区的硬分叉。通过链上治理公投实现：获批提案激活 runtime 替换——在单一块内用新 WASM 代码 blob 替换旧 blob，保持状态连续与运营。该路径减少停机与风险， 赋能社区随实际使用迭代完善协议。

随社区对系统信心增强，变更 runtime 的权力将显著收窄，以限制恶意控制升级流程时的攻击面。

治理体系

Quantus Network 通过 Substrate 继承 Polkadot 的 OpenGov 框架。代币持有人通过 **信念投票** 参与，将资产锁定不同时长以放大投票权重。放大倍数可从 1x（不锁定）到 6x（最长锁定）。 该设计通过将影响力与承诺绑定以鼓励长期一致。

提案按多条投票轨道「origins」分类。每条 origin 有定制参数，如批准阈值（例如高影响变更需绝对多数）、防垃圾最低押金、准备 / 执行期与决策时限以避免僵局。多轨道设计可并行处理从日常国库支出到关键 runtime 升级的各类公投。

Technical Collective 是由技术专家组成的精选团体， 作为专门机构提出、审查或白名单紧急技术事项， 通过专用轨道加速处理并保持社区监督。

Quantus 原样采用该体系，但初期采用极简配置以降低早期复杂度。最初仅启用 Technical Collective 轨道，用于协议升级或 参数调整等高权限约束性决策。

日后 Quantus 可增加非约束性社区投票轨道以探测对不可强制执行议题（如功能建议或生态调查）的民意。待公司将网络移交 DAO 后，该体系可变为有约束力。分阶段方法使网络可通过未来治理投票有机演进， 而不在一开始向用户强加不必要复杂度。

07

路线图

截至 2026 年的当前路线图，可能变更。

heisenberg inception 2024年12月	融资到位，选定 Substrate。
resonance alpha 2025年7月	公开测试网，Dilithium 签名，可逆交易。
schrödinger beta 2025年10月	功能完整，准备审计。
dirac beta 2025年11月	PoW 切换为 Poseidon2，处理审计意见。
planck beta 2026年1月	高安全账户，多签，硬件钱包，ZK 集成。
bell mainnet 2026年第二季度	主网上线。
fermi upgrade 2026年第四季度	ZK 证明聚合基础设施。

08

风险

构建 Quantus Network 存在固有风险。

实现问题

软件逻辑缺陷即使在设计良好的系统中也可能导致严重故障。

nist 算法选择问题

已选后量子标准（如 ML-DSA、ML-KEM）在标准化后可能暴露缺陷或后门。最坏情况下，此类缺陷可使攻击者通过公钥伪造签名推导私钥，构成链的灾难性失效模式。若缺陷公开，Quantus Network 可升级至新算法， 但若被低调利用可能永远无法 发现。

量子计算时间表

量子进展可能远晚于预期， 推迟 PQC 需求；反之，秘密开发（例如政府）若区块链社区 未能快速升级，可能带来突发威胁。

其他考量

一般采用障碍、金融 / 区块链监管不确定性以及加密生态固有的波动性。

09

参考文献与延伸阅读

[1] Shor, P. W. (1997). Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer. *SIAM Journal on Computing*, 26(5), 1484–1509. https://doi.org/10.1137/S0097539795293172

[2] Grover, L.K. (1996). A fast quantum mechanical algorithm for database search. *Proceedings of the Twenty-Eight Annual ACM Symposium on Theory of Computing*, 212-219. https://doi.org/10.1145/237814.237866

[3] Chainalysis. (2024). *The Chainalysis 2024 Crypto Crime Report*. https://www.chainalysis.com/blog/2024-crypto-crime-report-introduction/

[4] National Institute of Standards and Technology. (2024). *FIPS 204: Module-Lattice-Based Digital Signature Standard (ML- DSA)*. U.S. Department of Commerce. https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.204.pdf

[5] National Institute of Standards and Technology. (2024). *FIPS 203: Module-Lattice-Based Key-Encapsulation Mechanism Standard (ML-KEM)*. U.S. Department of

Commerce. https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.203.pdf

[6] Häner, T., Jaques, S., Naehrig, M., Roetteler, M., & Soeken, M. (2020). Improved quantum circuits for elliptic curve discrete logarithms. *arXiv:2002.12480*. https://arxiv.org/abs/2002.12480

[7] Gidney, C., & Ekerå, M. (2021). *How to factor 2048 bit RSA integers in 8 hours using 20 million noisy qubits*. *arXiv:1905.09749*. https://arxiv.org/abs/1905.09749

[8] Aggarwal, D., et al. (2021). Assessment of Quantum Threat To Bitcoin and Derived Cryptocurrencies. *ePrint IACR*. https://eprint.iacr.org/2021/967.pdf

[9] Roetteler, M., Naehrig, M., Svore, K. M., & Lauter, K. (2017). Quantum resource estimates for computing elliptic curve discrete logarithms. *arXiv:1706.06752*. https://arxiv.org/abs/1706.06752

[10] Open Quantum Safe Project. (n.d.). ML-DSA | Open Quantum Safe. Retrieved January 29, 2026, from https://openquantumsafe.org/liboqs/algorithms/sig/ml-dsa.html