# Quantus Network Whitepaper

**作者:** Christopher Smith | **最后更新:** 2026年1月14日

## 引言

### 量子威胁

传统区块链正面临量子计算问世带来的生存威胁。区块链的加密基础依赖于离散对数问题（DLP）的难度，而量子算法（特别是 Shor 算法）解决 DLP 的速度比经典计算机呈指数级增长。这种脆弱性可能使量子对手能够从公钥推导出私钥，从而伪造交易并解密敏感的财务数据。

其结果将是灾难性的系统崩溃。如果没有前瞻性的抗量子升级，价值数万亿美元的加密经济将面临此类攻击导致的突然贬值风险。

> 💡 **TIP**
>
> **Quantus 解决了这个问题。**

### 独特价值主张

Quantus Network 以拉丁语中意为"多少"的词命名，提供可扩展且量子安全的财富保全。
Quantus 不是一个智能合约平台。相反，就像一家没有菜单的高端餐厅，Quantus 专注于将少数几件事做得比任何其他 chain 都好。

具体而言，Quantus 使用：

- 所有交易均采用后量子 signature
- 采用后量子 signature 和加密（ML-DSA 和 ML-KEM）来保护对等节点连接
- 建立通往其他区块链的后量子 Bridge，并创建量子安全的包装代币（wrapped coins）
- 采用后量子 zero-knowledge-proofs 进行扩展
- 高安全性账户以威慑盗窃并支持从错误中恢复
- 易于阅读的 check-phrases，方便进行地址验证

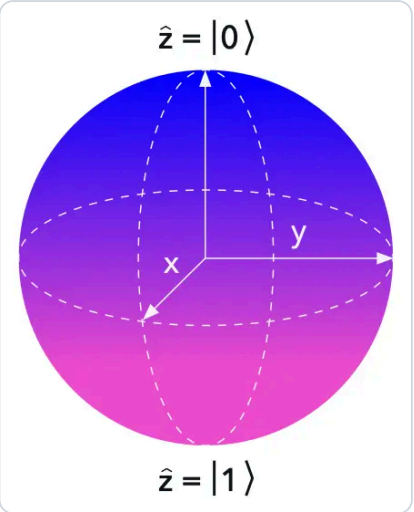
这种针对性的方法使用户能够自信地保全财富，将量子威胁转化为机遇。

> 💡 **TIP**
>
> Quantus 是您财富的未来堡垒。

# 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和纠缠等原理来执行经典机器难以处理的计算。




与只能是 0 或 1 的经典比特不同，量子比特（qubits）可以同时存在于多种状态，从而为某些问题提供指数级的并行处理能力。**这种能力对支撑区块链金融的加密系统构成了生存风险，因为为量子硬件开发的算法破坏了大多数公钥加密的安全性假设。**

### Shor 算法

由 Peter Shor 于 1994 年提出，为量子计算机分解大整数和解决离散对数问题提供了一种多项式时间方法。从本质上讲，它利用量子傅里叶变换（QFT）来寻找函数的周期，从而能够高效地逆转 RSA 或椭圆曲线加密（ECC）等方案基础的陷门函数。

**对于区块链金融而言，这意味着拥有足够强大量子计算机（估计约为 2,300 个逻辑量子比特）的攻击者可以在多项式时间 $O(n^3)$ 内从公钥推导出私钥。这是一种极端的加速，使脆弱的系统在一夜之间过时。**

### Grover 算法

由 Lov Grover 于 1996 年提出，为非结构化搜索问题提供了平方级加速，将从未排序数据库中查找特定项目的时间从 O(n) 减少到 O(√n) 次操作。它通过量子干涉迭代地放大目标状态的振幅来工作。虽然不像 Shor 算法对非对称加密那样具有毁灭性，但 **Grover 算法会影响对称原语，如哈希函数和 AES 加密，有效地将安全级别减半**（例如，256 位密钥在面对量子攻击时表现得像 128 位）。

虽然有影响，但这种攻击可以通过简单地将安全位数增加一倍来缓解，而无需更改加密方案。此外，Grover 的平方级加速由于其高量子比特和门要求而不切实际，需要数十亿次顺序操作，且并行化有限，即使在未来的硬件上，在现实世界中进行逆向计算也是不可行的。

## 量子计算对区块链金融的危险可分为四个领域：

### 伪造数字 signature

Shor 算法直接威胁到大多数区块链中使用的基于 ECC 的 signature（例如比特币的 secp256k1 曲线），允许对手冒充用户并授权欺诈交易。这种能力将代表区块链最基本功能的重大失败。

### 在零知识系统中伪造虚假证明

许多零知识证明，例如专注于隐私金融的 zk-SNARKs 中的证明，依赖于通过椭圆曲线配对实现的离散对数难度；Shor 算法可以创建看起来有效但实际无效的证明，这可能允许攻击者铸造新币或伪造 Layer-2 (L2) 的状态。

### 解密秘密信息

量子攻击可能会暴露 Zcash 或 Monero 等隐私协议中受脆弱公钥方案保护的加密数据。它还可以解密金融协议中的 p2p 通信，揭示敏感的财富细节并实现针对性的盗窃。

### 逆向哈希函数

Grover 算法可以加速对 SHA-256 等哈希值的原像攻击（用于工作量证明和地址生成），但这是最不令人担心的威胁。许多后量子加密方案都采用了基于哈希的结构，因为只要摘要足够大，哈希就被认为是足够安全的。

## 后量子加密中的扩展挑战

虽然后量子加密（PQC）提供了针对量子威胁的基本保护，但由于这些算法的固有设计，它引入了显著的扩展障碍。与依赖紧凑数学结构的椭圆曲线方案不同，PQC 原语需要更大的参数来维持对经典和量子对手的安全性。这导致公钥、私钥和 signature 显著变大，通常大出几个数量级。

下表说明了 128 位后量子安全级别的 ML-DSA 与 256 位 ECDSA 等经典对应方案的典型大小：

| 算法 | 公钥大小 (字节) | 私钥大小 (字节) | signature 大小 (字节) |
| --- | --- | --- | --- |
| ML-DSA-87 (Dilithium) | 2,592 | 4,896 | 4,627 |
| ECDSA (256-bit) | 32 | 32 | 65 |

**如表所示，ML-DSA signature 可能比 ECDSA 对应方案大 70 倍以上，公钥大 80 倍以上。**

其他 PQC 家族加剧了这一问题：基于哈希的方案（如 SPHINCS+）可能会产生高达 41 KB 的 signature，而即使是像 FALCON 这样经过大小优化的格方案变体，其大小仍是经典方案的数倍。

在区块链背景下，这些膨胀的大小会演变成系统性的扩展问题。更大的 signature 会使单个交易膨胀，随着区块迅速填满并需要更多时间进行验证，每秒交易量（TPS）会降低。这也会给对等（P2P）通信带来压力，增加带宽需求和传播延迟，从而在工作量证明等共识机制中增加网络分叉或孤立区块的风险。存储需求也会受到影响，导致更高的节点运营成本和参与障碍，特别是对于资源受限的用户或验证者。

**这些扩展挑战是所有区块链未来都必须解决的问题。例如，如果最大区块大小不增加，比特币的 TPS 将远低于 1。**

# Quantus Network 架构

## 后量子加密原语

Quantus Network 采用 **NIST 标准化的 PQC** 原语，以确保交易和网络通信免受量子威胁。交易完整性的核心是 **ML-DSA（基于模格的数字签名算法**，原名 CRYSTALS-Dilithium），这是一种基于格的签名方案，因其在安全性、效率和易实现性之间的平衡而被选中。**ML-DSA 利用了模格上的容错学习（LWE）和短整数解（SIS）等问题的难度**，为经典和量子攻击（包括 Shor 算法的攻击）提供了强大的抵抗力。

对于交易签名，**Quantus 集成了 ML-DSA-87**，这是提供最高安全级别（NIST 安全级别 5，相当于经典 256 位和量子 128 位安全性）的参数集，以**防范格问题中潜在的密码分析突破**。这一选择优先考虑了谨慎性，因为格密码学相对较新，且不像经典方案那样经过实战检验。更大的参数降低了格密码分析潜在进展带来的风险，而在较小密钥大小成为较弱目标时，它依然稳固。

### 替代方案

选择 ML-DSA 而非 FN-DSA (Falcon) 等替代方案的原因包括：

- FN-DSA 的实现复杂度更高（例如，需要浮点运算，这在区块链中并不友好）
- 其规范中缺乏确定性密钥生成
- 开发时其状态尚未最终确定

基于哈希的选项（如 SLH-DSA）因其更大的 signature 大小（超过 17 KB）而被否决。Substrate 内置了密码敏捷性（能够更换不同的签名方案），因此如果未来情况需要，添加这些替代方案相对容易。

虽然 ML-DSA-87 会导致更大的密钥和 signature，但在 Quantus 的早期网络中，这些是可控的，因为存储尚未成为瓶颈，且未来的优化（如通过零知识证明实现的 wormhole addresses）将解决扩展问题。

有关实现的更多技术细节，请参阅 QIP-0006。

### LibP2P

**Quantus Network 使用 ML-DSA 进行身份验证和 ML-KEM（基于模格的密钥封装机制，原名 CRYSTALS-Kyber）进行加密，以保护对等（P2P）节点通信。**

这种集成将 PQC 扩展到了 libp2p 网络栈，修改了核心组件以实现抗量子性：使用 ML-DSA-87 signature 进行对等节点身份识别，并使用 ML-KEM-768 进行传输安全（通过额外的 KEM 消息扩

展 Noise 握手，以实现抗量子的共享密钥）。

P2P 层在量子安全分析中经常被忽视。对等节点的身份验证很重要，但攻击者在对等节点级别能做的最坏事情就是冒充节点并发送无效消息，这可能导致拒绝服务。这种攻击已经通过以下事实得到缓解：在区块链模型中，节点通常是不受信任的，如果检测到攻击，节点可以轻松更换其密钥。同样，解密 P2P 通信给攻击者带来的收益有限（例如，跟踪交易路径，可通过代理或 Tor 缓解），且大多数数据最终都会在链上公开。

**尽管如此，对 P2P 层进行量子加密可以防止窃听、中间人攻击和量子解密，确保节点 gossip、区块传播和其他网络交互在可预见的未来保持机密且不可篡改。**

有关实现的更多技术细节，请参阅 QIP-0004。

## 扩展 PQC

为了应对后量子加密固有的扩展挑战，**Quantus Network 引入了一种创新的聚合后量子签名方案，称为"Wormhole Addresses"。** 该系统利用通过 Plonky2 证明系统（基本上是 STARKs）生成的零知识证明（ZKPs），将余额验证移至链外，允许链验证单个紧凑证明，而无需处理单个 signature。

**Wormhole Addresses 能够通过一个证明验证大量交易**，公共输入（如 nullifiers、存储根、退出地址和金额）成为主要的限制因素。这将分摊到每笔交易的存储需求减少到**每笔交易约 256 个额外字节，远小于任何已知的 PQC 签名方案。**

该方案的量子安全性源于使用安全哈希函数 Poseidon2 通过 FRI（快速里德-所罗门交互式预言机证明）进行承诺，而不是 SNARKs 中常用的量子脆弱的椭圆曲线配对。

此外，身份验证秘密隐藏在 Poseidon2 之后。由于安全哈希函数仅被 Grover 算法平方级削弱而不会被破解，哈希原像证明可以在 ZK 背景下充当轻量级的后量子签名，类似于 SPHINCS+ 等基于哈希的方案。

### 客户端 / 证明者流程

用户通过对盐（salt）与秘密（secret）的拼接进行双重哈希处理，生成一个可证明无法花费的地址：

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

这种构造防止了假阳性（例如，将单次哈希的公钥误认为无法花费的地址），因为在 Substrate（以及通常情况下）中，区块链地址是公钥的单次哈希，而公钥是通过某种代数运算从私钥推导出来的，而不是通过安全哈希。因此，该构造的安全性归结为寻找安全哈希的"原像的原像"。发送到此

地址的代币实际上已被销毁。它们无法被花费，因为接收它们的地址不存在私钥。因此，这些代币可以在不增加供应量的情况下重新铸造（re-minted）。

对于每次转账，都会创建一个 TransferProof 存储对象，其中包含唯一的全局转账计数等详细信息。用户的钱包从最近区块头的存储根生成到此 TransferProof 叶节点的 Merkle-Patricia-Trie (MPT) 存储证明。

计算 nullifier：

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

为了防止双重支出，秘密是从钱包种子中确定性推导出来的，以便保留。

### 聚合器流程

任何一方（客户端、矿工或第三方）都可以使用 Plonky2 的递归聚合多个证明，形成一个证明树，其中每个父证明都是对子证明的验证，且子证明的公共输入被聚合：

- nullifiers 保持不变传递
- 退出地址被去重
- 区块哈希被证明是链接的，然后除了最近的一个之外全部丢弃
- 重复退出地址的金额被累加 这种递归支持分层聚合，极大地减少了链上数据。

### 链 / 验证者流程

**网络通过检查以下内容来验证聚合证明：**

- 区块哈希在链上且为最近的
- nullifier 的唯一性（防止双重支出）
- 证明的有效性

**ZK 电路强制执行：**

- 存储证明的正确性
- nullifier 计算的准确性
- 地址的不可花费性
- 输入和输出之间的余额匹配
- 区块头的链接

**选择 Plonky2 的原因如下：**

- 已通过审计
- 后量子安全
- 无需信任设置（no trusted setup）
- 高效的证明/验证
- 无缝的证明聚合
- Rust 原生实现
- 兼容 Substrate 的 no-std 环境

### 性能亮点包括：

**170 毫秒内的递归证明和紧凑的大小**（每个聚合证明 100 KB），实现了吞吐量的巨大提升。

在区块大小为 5 MB 且所有交易都指向同一个输出的最佳情况下，**Wormhole Addresses 可以在单个区块中打包约 153,000 笔交易**（4.9 MB / 每个 nullifier 32 字节），比约 685 笔原始 ML-DSA 交易（5 MB / 每笔 7.3 KB）提高了 223 倍。

### 安全说明

潜在风险包括电路/验证实现错误导致的通胀漏洞，尽管如果重新铸造的代币超过了零发送地址的余额，这在经济上是可以检测到的。用户可以选择通过发布第一次哈希而不透露秘密来证明一个地址是 wormhole。验证交易是未经签名的，因此需要通过非财务手段缓解因交易失败导致的拒绝服务。代币供应量计算得以维持，因为重新铸造表现为新币，但通过销毁维持了最大供应量保证。

有关实现的更多技术细节，请参阅 QIP-0005。

## 共识机制

**Quantus Network 使用工作量证明（PoW）共识算法，该算法保留了比特币共识算法的理想属性，同时通过将 SHA-256 替换为 Poseidon2，提高了与 ZK 证明系统的兼容性。**

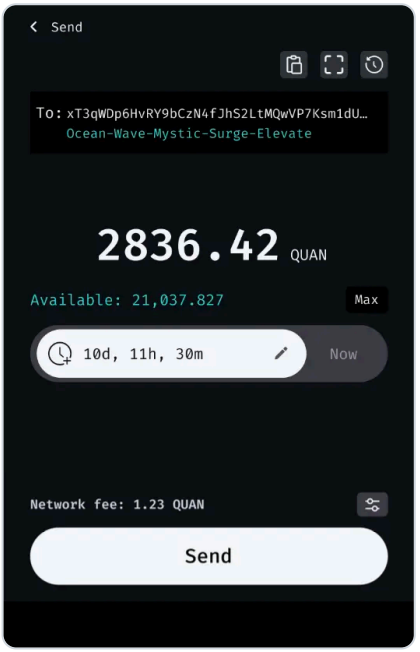
重要的是，这一更改并非为了量子安全。SHA-256 等加密哈希函数虽然会被量子算法（特别是 Grover 算法）削弱，但不会被摧毁。出于这个原因，一些后量子签名方案使用安全哈希作为构建模块。

Poseidon2 是 Poseidon 哈希函数的改进版。对于涉及 SHA-256 等传统哈希函数的计算，创建 SNARKs 或 STARKs 所需的门数通常是使用 Poseidon 的近 100 倍，后者完全依赖于域元素上的代数函数，而不是位级操作。我们为 Poseidon2 和 Plonky2 使用 Goldilocks 域，以最大限度地提高效率。

# 财富保全

**管理加密货币密钥存在许多风险。其中大多数是可以避免的。Quantus Network 将易用性融入链本身，使非专业人士也能安心交易。**

## 可撤销交易

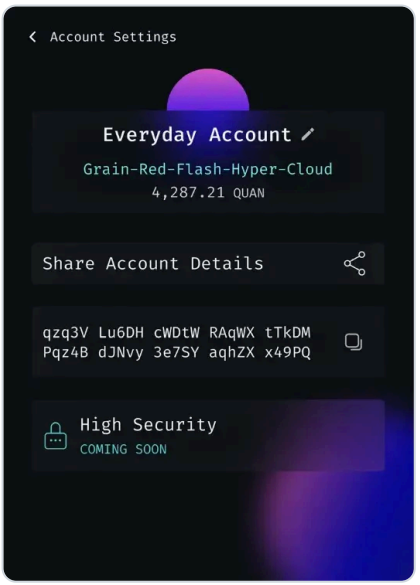



**Quantus Network 提供用户可配置的可撤销交易，允许发送者设置一个时间窗口，在此期间他们可以取消发出的转账，从而在不牺牲区块链核心不可逆性的情况下增强盗窃威慑和错误纠正。**该系统利用修改后的 Substrate“调度器托盘”（scheduler pallet），使用时间戳进行直观的延迟，允许客户端通过简单的界面安排转账，并在钱包中为发送者（带有取消按钮）和接收者（显示如果不取消则完成的倒计时）显示倒计时。这在商业的快速最终性与担心犯错或希望在没有托管服务的情况下进行诚信存款的用户灵活性之间取得了平衡。

**可撤销交易为新型安全协议提供了强大的构建模块，同时通过链上强制执行保持了去中心化。**

更多技术细节请参阅 QIP-0009。

## Check-Phrases

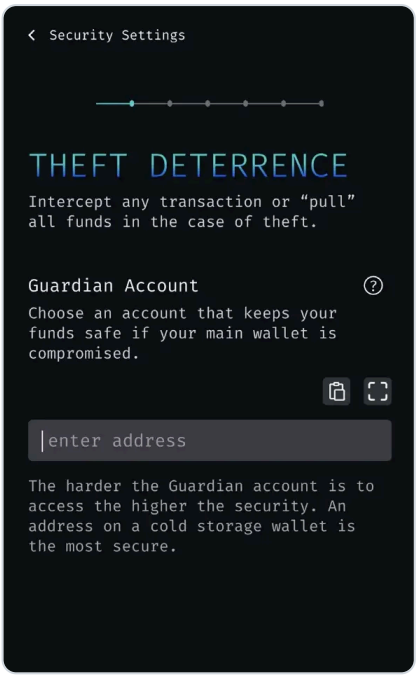



Quantus Network 引入了“check-phrases”，这是一种针对区块链地址和其他需要人工验证的数据的加密安全、人类可读的校验和。**通过对地址进行哈希处理，从 BIP-39 助记词列表中生成一串简短易记的单词，check-phrases 能够实现快速、防错的完整性检查，防止拼写错误、篡改和地址投毒（address poisoning）等攻击。** 该工具允许用户在转账过程中自信地验证地址，而无需依赖截断的显示或薄弱的校验和。使用 50,000 次迭代的密钥派生函数，以确保为给定校验和创建彩虹表的成本非常高。当然，对于大额交易，用户仍应手动检查地址的每个字母以确保正确。

更多技术细节请参阅 QIP-0008。

## 高安全性账户

Quantus Network 提供了将任何账户升级为“高安全性账户”的能力，该账户对所有发出的转账强制执行撤销期，允许指定的“监护人”（guardian）账户（如硬件钱包、多签账户，甚至是用户选择的受信任第三方）在撤销期内专门取消可疑交易，将资金发送给监护人而非发送者或接收者。这一选择性加入的永久功能建立在可撤销转账的基础上，用户在激活时指定延迟和拦截器，防止窃贼禁用它。




拦截器本身可以是另一个拥有自己监护人的高安全性账户，从而实现可组合的层级结构，其中每个监护人都对其保护的账户拥有更高的权限。这种设计模仿了传统金融中法院命令的撤销，但由用户控制。它在平衡高价值账户的安全性和便利性的同时，提供了检测和响应未经授权活动的时间，且不影响合法流程的区块链最终性。

更多技术细节请参阅 QIP-0011。

## 密钥恢复

许多加密财富已随其所有者一同入土。Quantus Network 提供了一种简单的方法来指定一个恢复地址，该地址可以在任何时候提取您的资金，但需遵守固定的延迟。在此期间，如果所有者拥有密钥，他们可以拒绝恢复。这一功能实现了生存性：用户拥有链上遗嘱，无需法院或遗产管理。

## HD-Lattice

分层确定性（HD）钱包是区块链的行业标准，允许用户为所有密钥备份一个助记词，相比于每次操作的手动备份，提高了安全性和便利性。

将此适应于 Dilithium 等格方案涉及两个挑战：

- HMAC-SHA512 的输出不能直接形成格私钥，格私钥需要通过拒绝采样获得“良好基”多项式。
- 非硬化密钥派生依赖于椭圆曲线加法，而格中缺乏这种加法（公钥在任何代数运算下都不封闭）。

Quantus Network 通过将 HMAC 的输出作为熵来确定性地构造私钥，而不是将其直接作为私钥本身，从而解决了第一个问题。第二个问题不太关键，格密码学是否可以适应解决该问题仍是一个开放的研究课题。

更多技术细节请参阅 QIP-0002。

# 代币经济学与治理

Quantus Network 存在于一个不断变化的环境中，我们不能假设我们在第一次尝试时就能做对所有事情。因此，我们选择一个简单的起点，并允许治理系统随着获得新信息而做出更改。这种设计使区块链成为一个能够随意适应环境的生命体。特别是，Substrate 治理流程允许在各个节点运行者之间进行极少协调的情况下对链进行深度更改。

## 区块奖励

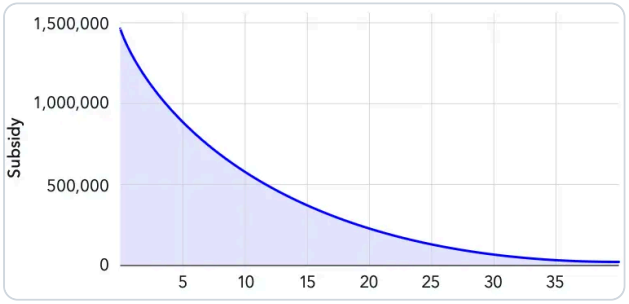
Quantus Network 采用模仿比特币的直接代币经济模型。最大供应量为 21,000,000 枚代币，简单的启发式方法决定了每个区块的奖励。

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

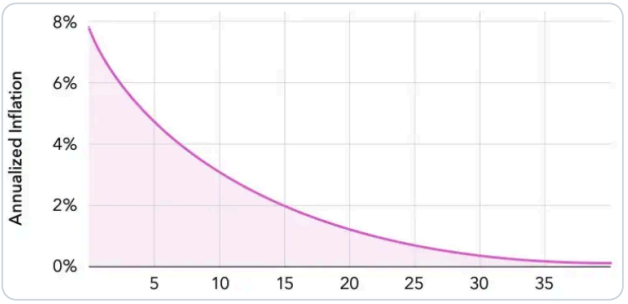
这种启发式方法形成了一条平滑的指数衰减曲线，因为区块奖励增加了当前供应量（current_supply），从而减少了下一个区块计算出的区块奖励。

任何来自手续费或其他方面的销毁都会减少当前供应量，并实质上成为区块奖励预算的一部分。常数的选择使得在没有任何销毁的情况下，99% 的代币将在大约 40 年内发放完毕。

**每年区块奖励**




**每年通胀率**




## 投资者分配

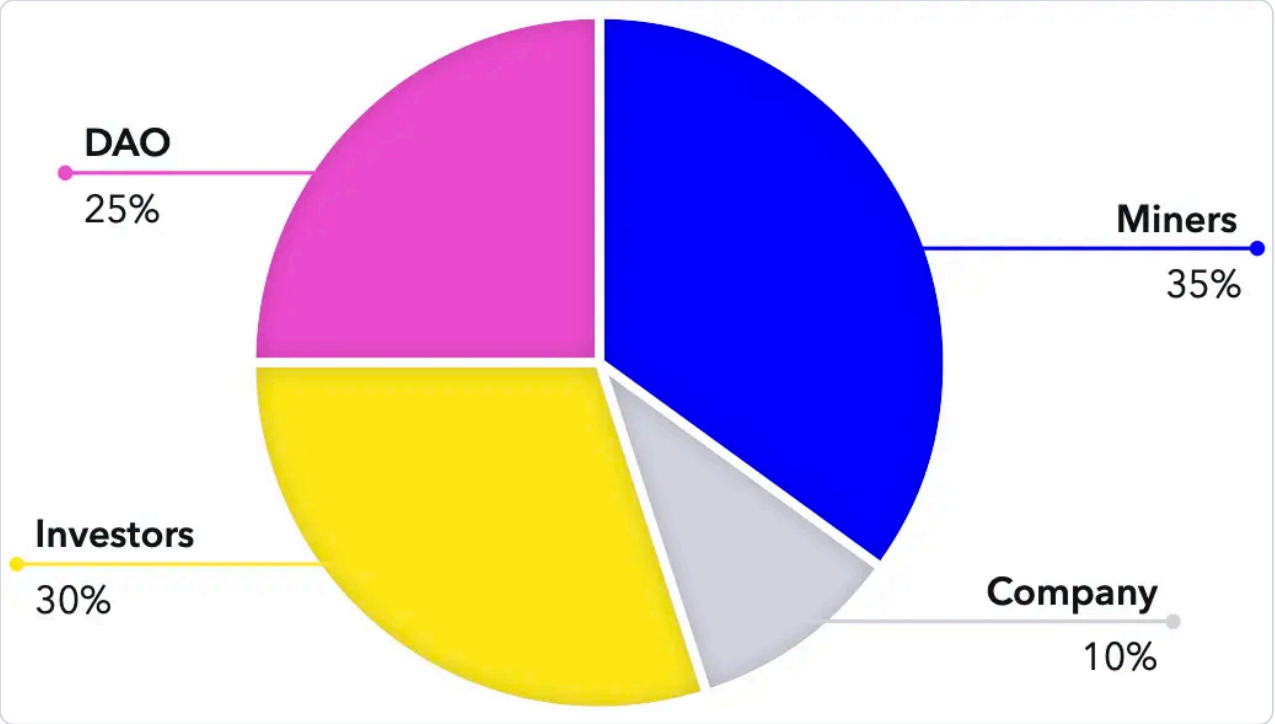
Quantus Network 是在天使投资者的帮助下建立的，他们在资助该项目时承担了巨大风险。为了避免投资者锁定期产生的供应压力，我们让所有投资者（无论是公开还是私人）在第一天就拥有流动性。这部分分配将是唯一的“预挖”。所有其他代币都必须通过挖掘产生。根据公开销售的成功情况，这部分将占总供应量的 20-30%。

## 公司分配

为了补偿团队在没有成功保证的情况下承担开发新技术的风险，我们将区块奖励分为两半。第一半归矿工所有。在大约四年的时间里，第二半归公司所有。这为公司提供了约占总供应量 10% 的事实上的归属计划。在此期间，矿工获得相同数量的新铸造代币。

此后，公司的区块奖励部分将转入由代币持有者治理的金库，实质上形成一个 DAO。

### 近似供应分配




## 交易手续费

标准交易将产生归矿工所有的手续费，从而提供包含交易的激励。来自高安全性账户的撤销交易将收取 1% 的按量手续费，该费用平分，一半归矿工，一半被销毁并进入未来的安全预算。通过 zk 聚合系统的交易也将收取 0.1% 的按量手续费，该费用将在矿工、证明聚合器和销毁之间分配。

## 无分叉升级

Quantus Network 通过 Substrate 的运行时（runtime）升级支持"无分叉"升级，允许区块链的核心逻辑（"运行时"）在不发生可能破坏网络或分裂社区的硬分叉的情况下进化。这是通过链上治理公投实现的，批准的提案会触发运行时切换，实质上是在单个区块中用新的 WASM 代码块替换现有的代码块，确保状态和运营的连续性。这种升级路径最大限度地减少了停机时间和风险，使社区能够迭代地完善协议。

## 治理系统

Quantus Network 通过 Substrate 继承了 Polkadot 的 OpenGov 治理框架。代币持有者通过信念投票（conviction voting）参与，他们同意在不同期限内锁定其资产，以放大其投票权重。这种放大范围从 1 倍（不锁定）到 6 倍（最大锁定）。这种设计通过将影响力与承诺挂钩来鼓励长期一致性。

提案被分类到称为"起源"（origins）的多个投票轨道中。每个起源都有定制的参数，如批准阈值（例如，高影响更改需要绝对多数）、防止垃圾邮件的最低存款、准备/执行期以及防止僵局的决策时间线。这种多轨道设计允许并行处理各种公投，从日常金库支出到关键的运行时升级。

技术委员会（Technical Collective）是由技术专家组成的精选小组，作为一个专门机构来提议、审查或将紧急技术事项列入白名单，通过专用轨道加快处理，同时保持社区监督。

Quantus 采用了这一系统且未做修改，但在早期阶段以简约的设置开始以避免复杂性。最初，只有技术委员会轨道处于活动状态，该轨道将用于具有约束力的高权限决策，如协议升级或参数调整。

稍后我们将引入非约束性的社区投票轨道，用于衡量对非强制性话题的看法，如功能建议或生态系统民意调查。当公司将网络移交给 DAO 时，该系统将具有约束力。

这种分阶段的方法允许网络通过未来的治理投票有机地进化，而不会在开始时给用户增加不必要的复杂负担。

# 路线图

## Heisenberg Inception

2024 年 12 月

**资金到位，选定 Substrate**

## Resonance Alpha

2025 年 7 月

**公开测试网，Dilithium 签名，可撤销交易**

## Schrödinger Beta

2025 年 10 月

**功能完备，准备审计**

## Dirac Beta

2025 年 11 月

**PoW 更改为 Poseidon2，处理审计问题**

## Planck Beta

2026 年 1 月

**高安全性账户，多签，硬件钱包**

## Bell Mainnet

2026 年第一季度

**主网上线**

## Fermi Upgrade

2026 年第二季度

**ZK 聚合**

# 风险

建立 Quantus Network 伴随着固有风险。

- **实现问题：** 即使是设计得最好的系统，软件逻辑中的缺陷也可能导致严重的故障。
- **NIST 算法选择问题：** 所选后量子标准（如 ML-DSA、ML-KEM）中可能存在潜在缺陷或后门，这些缺陷可能在标准化后出现。在最坏的情况下，此类缺陷将允许攻击者通过从公钥推导私钥来伪造 signature，这代表了链的灾难性故障模式。如果此类缺陷被公开，Quantus Network 可以升级到新算法，但如果此类缺陷被谨慎利用，它们可能永远不会被发现。
- **量子计算时间线：** 量子突破可能比预期晚得多，从而推迟对 PQC 的需求；相反，秘密开发（例如由政府进行）如果区块链社区未能迅速更新，可能会导致突然的威胁。
- **其他考虑因素：** 通用的采用障碍、金融/区块链领域的监管不确定性，以及加密生态系统固有的波动性。

# 结语

QUANTUS

我们相信开放协议、工作量证明和主权所有权的力量。Quantus Network 应用程序可在桌面和移动设备上使用，让用户能够存储数字资产、挖掘新区块，并在没有中间人的情况下参与更公平的金融未来。

我们致力于透明度、隐私，并通过安全的自托管工具赋予个人权利。