qubic whitepaper

QUBIC：一个用于 AI 驱动应用的扩展网络

qubic.org | 版本 1

免责声明

本白皮书仅用于信息目的，并不构成财务、投资、法律或其他专业建议。本文件中的内容按“原样”提供，不附带任何明示或暗示的保证。读者应在做出与本文件所述项目相关的任何决定之前，咨询自己的顾问并进行独立研究。

前瞻性声明

本白皮书可能包含前瞻性声明，包括但不限于预期的功能、技术、采用或其他项目目标。此类声明受风险、不确定性及其他因素的影响，可能导致实际结果发生重大差异。前瞻性声明的包含不应被视为对表现或结果的保证。

不构成投资建议

本文件不构成出售任何金融工具、证券或代币的要约，也不构成购买任何金融工具、证券或代币的邀请。代币的购买或持有涉及风险，包括但不限于价值损失的可能性。本文件中描述的代币不应被视为投资或传统投资的替代品。

监管风险

加密货币、代币和区块链技术的监管环境正在迅速变化。该项目可能会受到未来法律、法规或政府当局采取的行动的影响。无法保证该项目在任何特定司法管辖区内的合法性或监管待遇。

无准确性保证

尽管已尽一切努力确保本白皮书中所提供信息的准确性和完整性，但仍无法保证信息的可靠性或及时性。本白皮书可能会根据需要更新或修订，恕不另行通知。

司法管辖区限制

由于法律、法规或其他原因，参与此项目在某些司法管辖区可能受到限制。读者有责任了解并遵守其司法管辖区内适用的任何此类限制。

风险披露

参与区块链和加密货币项目涉及风险，包括但不限于财务损失、技术故障和市场波动。参与者被鼓励在参与项目前充分了解与项目相关的风险。

责任限制

在任何情况下，本项目的创建者、开发者、贡献者或关联方均不对因使用或依赖本白皮书包含的信息而导致的任何直接、间接、偶然或后果性损害承担责任。

通过访问和审阅本白皮书，您确认并同意本免责声明中的条款。如果您不接受这些条款，您应该避免与本白皮书所述的接触。

摘要

通用人工智能（AGI）的发展面临重大挑战，特别是对庞大计算资源的需求以及与这种强大技术集中控制相关的风险。集中式AI模型表现出明显的可扩展性和效率限制，这可能会减缓甚至阻止AGI的进展。同样，区块链网络在实现真正的去中心化、高效的共识机制和可持续的经济模型方面仍面临持续障碍。成熟的平台往往存在交易成本高、延迟问题和由于能源密集型共识协议造成的环境影响等问题，所有这些都阻碍了可扩展性和长期可行性。本文介绍了Qubic，这是一个第一层区块链网络，旨在通过创新的经济机制和去中心化治理模型解决这些挑战

Qubic采用基于多数同意的共识算法，无需交易费即可实现亚秒级交易最终性。其经济模型结合了有用工作量证明（UPoW），将计算工作与有意义的任务相结合，例如通过Aigarth（一个在Qubic网络上运行的本地去中心化AI）进行分布式AI模型的训练和验证。这种经济结构激励网络参与并通过通缩机制促进可持续性。我们提供了对Qubic网络基础设施的详细分析，强调在裸机硬件上部署和优化节点通信协议，以进一步提高性能和安全性。探讨了共识协议的技术基础，说明了如何维护网络完整性并阻止恶意活动。在潜在攻击向量的背景下，详细阐述了加密技术和安全措施。此外，我们讨论了Qubic与Aigarth的集成如何实现去中心化AI计算，为在分布式和安全环境中发展AGI做出贡献。我们展示了Qubic对构建一个去中心化、高效和可持续的区块链网络所做的贡献，该网络能够支持AGI的发展。

这项工作：

(a) 讨论了区块链中治理、经济模型和去中心化的固有问题，以及AGI开发所需的计算要求和风险。

(b) 解释了Qubic的经济机制，如有用工作量证明（UPoW）、经济和激励结构，以及其使用多数共识和拜占庭容错的去中心化治理模型。

(c) 提供了网络基础设施的深入描述，涵盖裸金属部署、节点间通信、智能合约执行以及支持Qubic的一切——性能、安全性和通过Aigarth支持AGI相关计算的能力。

(d) 提供了共识协议及其安全特性的技术描述，展示了它们如何保持网络完整性。

(e) 描述了支撑 Qubic 可持续经济模型的硬币分配、发行时间表和通缩机制。

(f) 描述了 Qubic 中用于应对潜在安全挑战的密码学基础原理和技术。

(g) 不描述人工通用智能计划 Aigarth，因为关于 Qubic 的 AI 能力的新科学出版物将随后发布。

注意：Qubic 正在积极开发中。有关持续研究和更新，请访问我们的网站 www.qubic.org，并可通过 info@qubic.org 向我们发送评论或建议。

目录

1

介绍

区块链技术因其能够提供去中心化、安全和透明的基础设施而备受赞誉。然而，重大挑战阻碍了其广泛采用。当前的Layer 1网络，利用工作量证明（PoW）和权益证明（PoS）等共识机制，面临着可扩展性限制、高交易成本以及经济可持续性等问题。这些传统方法的特点是能源消耗过度、交易吞吐量受限以及可访问性障碍复杂（Zolfagharinejad等人，2024年）。因此，开发者在追求高效、可扩展和真正去中心化网络的过程中，越来越认为需要进行根本性重新设计。

与此同时，人工智能的快速发展——尤其是朝着通用人工智能（AGI）的方向——揭示了巨大的计算需求，导致资源集中在大型强大的数据中心中。这种集中化引发了伦理和安全问题，因为少数实体的AGI控制可能垄断人类最变革性技术之一（Zolfagharinejad等人，2024年）。像OpenAI这样的组织 exemplify 了这一困境；实现AGI所需的巨大计算能力和资源突显了透明度、包容性和控制的局限性。此外，随着模型复杂性的增加，对计算效率和可扩展性的需求呈指数级增长。当前架构严重依赖GPU进行并行处理，但在处理序列AI任务时遇到效率瓶颈（Zolfagharinejad等人，2024年）。

这些交织的挑战催生了对一种能够通过优先考虑去中心化、计算效率和透明性来高效支持 AGI 的区块链的迫切需求。这样的解决方案将克服区块链技术的传统局限性，并解决 AI 开发中集中化的弊端。

从这两个双重需求中——重新构想区块链结构和开发可持续的、去中心化的 AGI——诞生了 Qubic 的愿景。在区块链创新先驱 Come from Beyond (CfB) 的指导下，CfB 引入了基于 NXT 的第一个权益证明 (Proof-of-Stake) 协议，并共同创立了 IOTA 中的初始有向无环图 (Directed Acyclic Graph, DAG) 结构，Qubic 为这些复杂问题提供了一种集成方法。借鉴 CfB 在去中心化、可扩展性和安全性方面的丰富经验，Qubic 的共识架构和经济模型直接受到了影响。这使 Qubic 成为一个旨在促进区块链技术和 AGI 可持续发展的解决方案。

1.1 问题陈述

当前的区块链领域存在一些挑战，限制了其作为 AGI 等高级应用平台的潜力。

- 可扩展性和效率约束：大多数第一层网络受到低效共识算法和网络延迟的困扰，这削弱了提高交易吞吐量和最终性的潜力。实时应用大多受到PoW和PoS算法限制，减缓高频交易，并使所有交易费用变得高昂，尤其是在高峰使用时段。

- 能源消耗和经济可持续性：传统的PoW网络仅对计算能力进行奖励，导致大量能源消耗而没有有用的计算输出。另一方面，PoS模型存在将奖励集中到更富裕参与者的风险，使网络可及性降低，并增加了少数人控制网络的可能性。在许多区块链系统中，可持续经济仍然是一个悬而未决的问题，其显著的通胀压力或治理结构使大量代币持有者偏袒。

- 治理和安全：平衡去中心化治理与强大的安全性仍然具有挑战性。许多网络采用的风险集中决策的模型，同时还要应对恶意攻击的脆弱性和决策过程中的低效性。

- 集中控制和计算能力：目前AGI开发需要大量的计算资源，只有财力雄厚的集中化实体才能负担得起。这也可能导致AI开发形成“围墙花园”，不允许更大社区参与。AGI日益增长的计算需求，提高了对可扩展、去中心化系统的需求，这些系统能够支持高级AI。

从上述挑战中可以看出，我们需要一个能够改进传统第一层效率的区块链网络，并为去中心化社区协议环境中的AGI独特计算需求提供结构支持。

在去中心化社区协议的环境中，AGI的计算需求是独特的。

1.2 Qubic解决方案概述

Qubic为这些挑战提供了一种整体解决方案，将新颖的经济机制和有效的治理引入Layer 1网络，以支持去中心化AGI的发展。Qubic方法的最重要元素是：

1. 共识算法：

Qubic采用基于拜占庭容错原则的基于多数的共识机制，以积极确保网络的安全可靠运行。基于包括Nick Szabo和Leslie Lamport在内的研究人员最初提出的底层多数原则，该系统设计为在去中心化治理框架内提供容错和安全性（Szabo，1997；Lamport等人，1982）。

网络正在使用一个包含676个实体的共识系统，这些实体被称为Computors。为了就交易的效性达成一致，该网络需要至少451个这些Computors同意。这与认为容错系统需要在多数之间有一些交集以确保对恶意节点的弹性的多数系统方法一致。

共识系统可以使用"好"和"坏"的联盟来定义，其中任何好共识都与其他共识显著相交以确保一致性，即使在存在坏联盟的情况下也是如此。这种结构确保没有任何单个恶意联盟能够控制网络的决定。Qubic的共识大小阈值满足共识系统以下传播标准：

$$Q > \frac{N + F}{2}$$

(Castro 和 Liskov，1999)

Where Q 是仲裁大小，N 是 Computors 的总数，F 是可容忍的最大故障节点数。通过设置 Q=451 和 N=676，Qubic 确保了鲁棒性，满足在最多三分之一故障节点的情况下维持共识的标准

$$F \approx \frac{N - Q}{2}$$

这种仲裁设计通过以下方式提高了 Qubic 的安全性和治理完整性：

- 拜占庭容错：确保网络能够在某些节点表现出任意或恶意行为的情况下容忍并正常工作。

- 防止中心化：防止任何单一实体在共识过程中占据主导地位，由仲裁者（第3.2.3节）强制执行。

- 扩展容错：抵抗集中控制和协调的恶意攻击。

2. 有用工作量证明 (UPoW)：

Qubic 引入了一种有用工作量证明机制，重新定义了挖矿以使计算工作与生产任务相一致。与传统 PoW 系统不同，后者消耗大量能源却未对计算进度（除保障区块链安全外）做出贡献，UPoW 将资源用于 Aigarth AGI 计划中优先级高的 AI 任务。

UPoW 的关键方面包括：

- 资源效率：通过执行对 AI 模型的训练和发展有意义的计算工作来避免浪费。

- 包容性：允许基于 CPU 的参与，因此有可能拥有更广泛的 AGI 开发者群体。

- 网络目标的协同：将挖矿工作导向有利于网络及其所有参与者的活动，代表了区块链系统资源利用方式的范式转变。

3. 硬件部署以提高性能和安全性：

为了确保卓越的性能、安全性和去中心化，Qubic直接在裸金属硬件上运行，而不是依赖传统的操作系统或虚拟机。

这一架构决策体现了Qubic对效率和弹性生态系统的承诺。

裸金属部署的主要优势：

- 卓越性能：通过消除操作系统层的开销，裸金属部署允许 Qubic 直接访问硬件资源，实现更快的交易处理和更低的延迟。

- 增强安全性：在不依赖传统操作系统的情况下运行，减少了软件环境中常见的漏洞，显著降低了远程攻击的攻击面。

- 可靠性：简化的硬件级操作最大限度地降低了第三方软件引起的风险，确保稳定和可预测的环境。
- 对去中心化的承诺：部署和维护裸金属节点的努力和专业知识构成了自然的进入壁垒，吸引高度投入的参与者，并降低恶意或随意操作者的风险。

4. 去中心化经济模型：

Qubic经济学旨在激励网络中的长期参与和稳定性，采用平衡的经济模型。QUBIC币是激励网络参与者的原生货币，特别是支持网络共识的Computors。

经济模型的特点包括：

- 激励对齐：根据参与者对网络内计算任务贡献的价值来支付参与者。

- 通缩机制：通过实施币燃烧或其他通缩策略，随着时间的推移逐渐减少流通供应量，增加稀缺性。

- 经济可持续性：努力在奖励参与者与保持网络经济健康之间取得平衡，以确保在所有角色中都能进一步吸引参与和投资。

5. Aigarth的可扩展、透明的AGI框架

Qubic的UPoW模型生成计算输出，使Aigarth受益，Aigarth是一个用于去中心化AGI创建的项目。虽然Aigarth利用了Qubic的输出，但它是一个自给自足的实体，使用Qubic网络中产生的计算解决方案，在分布式CPU上运行其AI活动，而不是依赖GPU的集中式基础设施。

该模型的关键要素包括：

- 去中心化AI开发：通过让广泛的贡献者社区参与AGI开发，降低集中控制的风险。

- 受大脑启发的处理方法：利用模拟人类认知过程的序列处理方法，使计算方法与自然智能模型保持一致。

- 可持续扩展：在不集中控制或对能源资源造成不当负担的情况下，满足更大的计算需求。

- 伦理对齐：通过在文献中解决伦理问题，确保通用人工智能（AGI）的开发是透明的、可访问的，并专注于集体利益。

通过这种资源共享关系，Qubic 提供了去中心化的计算框架，Aigarth 利用该框架来执行复杂的 AI 任务。这种设置使 Qubic 能够专注于区块链的可扩展性和安全性，而 Aigarth 则通过应用 Qubic 的去中心化计算结果继续在 AI 领域发展。

2

网络基础

本节解释了 Qubic 的经济机制和共识协议，这些机制和协议旨在支持安全、去中心化和高效的网络操作。我们讨论 Qubic 的实用工作量证明（UPoW）、经济、激励结构以及治理模型。

2.1. 经济机制

2.1.1. 有用工作量证明 (UPoW)

有用工作量证明 (UPoW) 模型代表了 Qubic 的一项关键创新，它通过将计算能力导向有意义、以 AI 为中心的任务，将其与传统的 Proof of Work (PoW) 框架区分开来。在 UPoW 中，计算资源被用于解决有生产力的难题，例如训练有助于 Qubic 人工通用智能 (AGI) 计划 Aigarth 的人工神经网络 (ANN)。这种转向有目的的计算解决了能源消耗问题，并将矿工的贡献与网络更广泛的目标——推进 AI——相一致。有关 PoW 系统和能源效率的更多信息，请参见 (Beiko, 2021)。

有目的的计算

UPoW 将计算能力导向用于 AI 模型的训练和验证，直接服务于 Aigarth 计划的目标：去中心化 AGI。与在任意密码学难题上浪费计算资源的传统 PoW 系统不同，UPoW 将挖矿工作与有用任务相一致。Beiko (2021) 等关于区块链系统能源效率的研究支持这种方法，表明将计算工作导向有生产力的目标可以显著减少浪费。

能源效率

UPoW 通过将计算任务导向训练 AI 模型而非解决任意谜题来减少能源浪费。近期关于可扩展计算系统的研究（Zolfagharinejad 等人，2024）表明，这种将高能耗工作负载转移的做法具有环境效益。

挖矿与奖励框架

在 Qubic 中，挖矿过程将计算贡献与有意义和有生产力的任务相结合，这与专注于最大化哈希率的传统工作量证明（PoW）系统形成对比。Qubic 挖矿者的计算能力由其处理速率衡量。

H_m, 以每秒迭代次数 (it/s) 进行量化。这反映了矿工硬件每秒可以执行的计算操作数量。然而，效率因子 E,

表示找到有效解决方案的概率，以确保质量解决方案仍然是重点。

Qubic中的挖矿是适应性和相对的。找到解决方案的可能性在所有矿工之间均匀分布，无论计算任务的复杂性如何。这确保了：

- 公平性得到保留：所有矿工，无论硬件复杂性如何，都面临相称的挑战。
- 排名保持稳定：Computors（以及矿工的贡献）的相对排名不受任务复杂性的影响。

如果计算任务变得更加具有挑战性，所有参与者的“最低分数”（解决方案提交率）会同等程度地降低。然而，相对排名和奖励分配保持一致，这鼓励了公平性和参与。这种适应性模型确保了公平的竞争环境，同时推动有意义的AI成果。

解决方案提交率反映了矿工的有效输出和计算效率。它按以下方式计算：

$$S_{rate} = H_m \times E$$

在哪里：
S_{rate} = 每秒提交的有效解决方案。
H_m = 矿工的哈希率（每秒迭代次数）。
E = 效率因子（每次迭代的有效解决方案）。

此指标激励矿工优化其硬件和算法，以贡献计算任务，而不是像 PoW 系统中那样简单地最大化原始哈希率。

对PoW能源效率的研究表明，更高的处理率结合优化的硬件和算法可以提高有效解决方案提交的速率，从而增加网络贡献和个人矿工的成功率（Beiko，2021；Zolfagharinejad等人，2024）。

UPoW 的运营动态

通过UPoW，Qubic激励矿工完成具有实际成果的计算任务，这与传统PoW系统形成对比，在传统系统中，计算工作被用于解决随机的密码学难题。UPoW通过将挖矿活动与Qubic的AGI发展目标相结合，提供了实际价值。这种模式提高了能源效率并推动了人工智能的进步。

UPoW 的关键方面包括：

- 有目的的计算：矿工为 AI 模型的训练和优化做出贡献，确保消耗的能量直接支持 AI 研究和开发中的有意义成果。

- 激励一致性：通过优先处理有用任务和维护不同复杂度下的公平性，Qubic 确保其挖矿模型既推进了区块链生态系统，也促进了 AGI 的发展。

- 包容性和可访问性：通过使任务适用于各种硬件，包括通用 CPU，UPoW 降低了矿工的进入门槛，促进了去中心化并减少了硬件垄断的风险。

- 能源效率：将计算能力重新定向到有用任务中，可以减轻传统 PoW 挖矿相关的环境影响。

与 PoW 不同，矿工负责保障网络安全，而 Qubic 则使用其一致性共识机制来实现这一点。这使得 Qubic 的 UPoW 模型能够将挖矿转变为一个有利于人工智能更广泛领域的进程，而无需矿工保障区块链安全。矿工通过 Aigarth 积极地为通用人工智能 (AGI) 的发展做出贡献。

这种方法创造了一个正反馈循环，其中挖矿参与的增加增强了网络的计算能力，从而推动人工智能的更快发展。反过来，通用人工智能 (AGI) 的进步可以改进网络功能，并在 Qubic 生态系统中开辟新的创新途径。

通过优化 UPoW 模型及其运行机制，本节重点介绍了 Qubic 如何有效地将区块链安全与有意义的计算工作相结合。UPoW 机制不仅解决了传统挖矿的效率问题，还通过策略性地利用矿工参与来推进 AGI 的发展，使个人利益与集体进步保持一致。

2.1.2 经济学

QUBIC 代币是 Qubic 网络经济中的能量单位，通过协调参与者之间的利益来保障和扩展生态系统。作为主要的交易媒介，QUBIC 代币促进交易、激励参与，并维持网络的增长和稳定性。它奖励 Computors 运行网络及其对网络安全做出的贡献。这种设计确保网络资源得到高效利用，同时支持平台的 AI 目标，与去中心化网络中有效的代币设计和激励机制的研究见解（Narayanan 等人，2016 年）保持一致。

排放结构与通缩机制

QUBIC币的排放结构遵循一个精心管理的计划，旨在
奖励计算和验证工作，同时保持长期经济
稳定性。由于总量有限，网络采用定期币销毁
机制，例如年度减半和特定的智能合约操作，以减轻
通货膨胀压力。这种方法与经济学中既定的原则相一致，该原则
强调控制发行和通货紧缩，以提高币值并鼓励长期
持有（Yli-Huumo 等人，2016 年）。

控制发行计划币燃烧机制（将在第 6.1 节中进一步讨论）是维持网络长期稳定和价值的基础。这些机制调节流通供应并激励持续参与，与 Qubic 的更广泛经济模型相一致，并促进可持续和平衡的生态系统。

计算器和矿工的奖励分配

在每个时代，表现高性能标准的计算器会从计划排放中获得 QUBIC 币的奖励。这种激励机制促进了持续的参与，并加强了网络安全和治理的贡献。奖励分配策略呼应了其他区块链系统中观察到的模型，其中积极参与直接与网络奖励挂钩，从而通过经济激励强化稳定性。

矿工，在UPoW框架内提供计算解决方案，根据与Computors达成的单独协议获得奖励。这些协议

本身不由Qubic协议强制执行，而是依赖于每个Computor与其关联矿工之间设定的相互条款。

经济学研究表明，将代币分配直接与网络健康和参与者表现挂钩的模型能够培养稳健且积极参与的社区，从而增强网络的长期可行性（Beiko，2021）。QUBIC代币作为Qubic网络中的主要价值单位，有效地协调了生态系统中的激励措施，以支持网络增长、安全性和计算生产力。

2.1.3 激励结构

Qubic的激励结构经过精心设计，旨在通过直接奖励Computors和间接激励矿工来使网络参与与期望行为保持一致。该系统确保了计算资源的有效利用，矿工和Computors都为网络的整体目标做出贡献（Gabuthy，2023）。通过结合个人和网络范围的奖励，这些激励机制鼓励矿工最大化其性能，并在各种Computors中有效贡献。这些机制支持去中心化AGI开发并强化网络。

个人奖励和网络贡献

Computor奖励和贡献评分：在每个时代中，Computors和Computor候选人（在公式下方称为Identities）通过从相关矿工那里积累有效解决方案来竞争，以获得资格留在下一个时代或成为其中之一（676个Computors）。

优化了他们设置的矿工提供了更高的计算贡献，帮助了Computors在后续的纪元中合格的机会。

每个计算器的奖励分配：在每个时代结束时，该时代的计算器将根据其在时代中收集的收益积分点获得总排放量的一部分作为收入。收益积分点是根据计算器性能指标计算的，这些指标激励节点提供高质量的服务，例如高网络连接性和处理速度。由于网络排放可能根据基于共识的治理决策（如销毁合约和捐赠分配）而减少，因此计算器的收入可能会进行调整。

跨多个身份的总奖励：矿工可以灵活地将他们的计算工作分配到一个时代内的多个计算器中。这鼓励解决方案的策略性分配，从而最大限度地提高矿工在整个网络中的潜在奖励。

在本节中，我们概述了个人和网络奖励的结构，读者可以在第6.3节中找到有关Qubic经济模型如何促进网络安全和参与性的更多细节。

2.2 共识框架

Qubic的共识框架建立了一个安全、去中心化的系统，通过创新的共识机制确保网络完整性。通过整合Quorum共识算法和拜占庭容错（BFT），Qubic即使在去中心化、易出故障的环境中也能保持可靠运行（Lamport等人，1982年；Castro & Liskov，1999年）。

2.2.1 Quorum共识算法

Qubic中的Quorum共识算法使分布式参与者（称为Computors）能够集体验证计算任务。这种方法对于网络的有用工作量证明（UPoW）模型至关重要，确保了计算效率，同时提供了对错误或恶意节点的弹性（Szabo，1997年）。

共识委员会数学基础

1. 共识委员会选择：

共识委员会代表整个网络中足以执行计算验证的Computors子集。在Qubic中，Computor是一个可以部署在一个或多个物理节点上的逻辑实体。然而，在任何时候，网络中每个Computor只允许一个活动节点，而托管Computor的其他节点可以作为备用参与网络，如果需要，随时准备替换主节点。这种方法增强了网络的容错能力，并有助于保持网络稳定性，确保共识委员会参与的高可用性。

此外，单个节点可以托管多个Computors。通过将Computors的数量与物理服务器的数量解耦，Qubic允许可扩展性和灵活性。

从数学上讲，如果N表示网络中Computors的总数，那么为了容忍f个有故障的Computors（Lamport等人，1982年），其中：

$$f \leq \frac{N-1}{3}, \text{ the quorum size } Q \text{ must satisfy:}$$

$$Q \geq 2f+1$$

(Castro & Liskov, 1999)

对于由$N = 676$个Computors组成的Qubic网络，系统设计为能够容忍高达

$$f = \frac{N-1}{3} = 225 \text{ faulty Computors}$$

因此，共识大小必须至少为：

$$Q \geq 2 \times 225+1 = 451$$

该标准确保共识中包含足够数量的诚实Computors，即使在拜占庭故障存在的情况下也能达成共识，从而在网络中断或恶意活动存在时仍能实现可靠共识。

2. 投票机制：

每个N计算器（Qubic网络中的676个计算器）独立执行分配的计算任务，然后对结果进行投票。如果至少Q个计算器对结果达成一致，则形成共识。

Let:

- N代表网络中计算器的总数。
- Q表示达成共识所需的同意 Computors 数量。当满足以下条件时达成共识：

$$\sum_{i=1}^{N} v_i \geq Q$$

其中 v_i 是 Computor i 的单个投票，要么支持 $(v_i = 1)$，要么反对结果 $(v_i = 0)$。

鉴于：

$$Q \geq 2f + 1$$

其中 f 是网络可以容忍的最大故障或恶意 Computors 数量，这种多数投票机制对于维护网络稳定性和高效决策至关重要。它确保了约定的结果得到三分之二以上多数成员的认可，符合 BFT 要求。

3. 共识最终确认：

一旦多数达到共识，结果将被接受并记录在网络中。Qubic 的共识算法依赖于一种简单的基于多数的方法，通过利用大量 Computors 来验证和确认计算（Narayanan 等人，2016 年），确保共识质量。这种方法通过强调共识过程中的广泛参与和冗余来增强网络的鲁棒性。

以下图表说明了传统与去中心化信任系统，并有助于理解 Qubic 的方法。

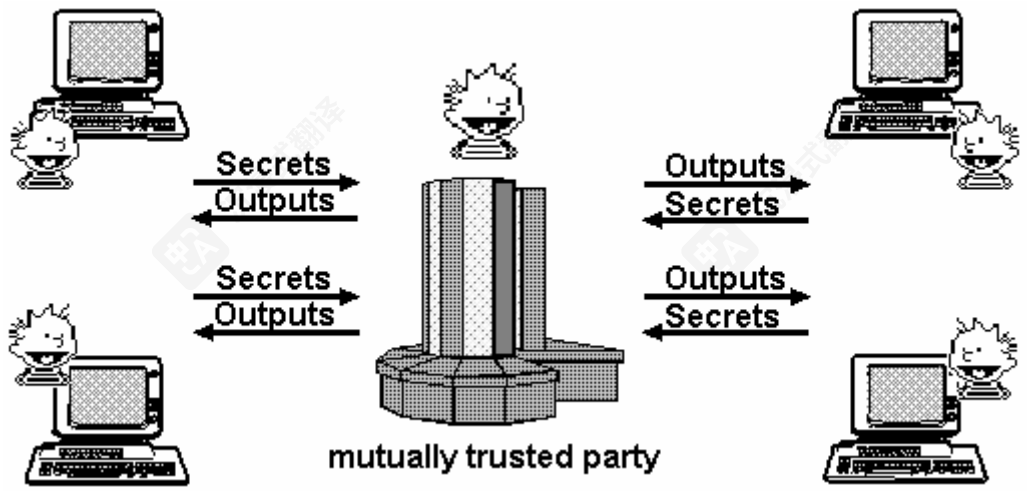

图*1*： 传统集中式信任模型。来自 (Szabo, 1997)

该图表示一个传统的集中式模型，其中单一、相互信任的方调解节点之间的交互。这种方法集中控制权和

决策，可能存在单点故障的风险。这种模型容易受到信任和安全问题的困扰，因为中央权威可能失效或采取恶意行为。

Qubic的方案：Qubic通过其共识机制在多个节点间分配信任，避免了这种中心化，从而减少对单一权威的依赖，并增强了安全性和容错能力。

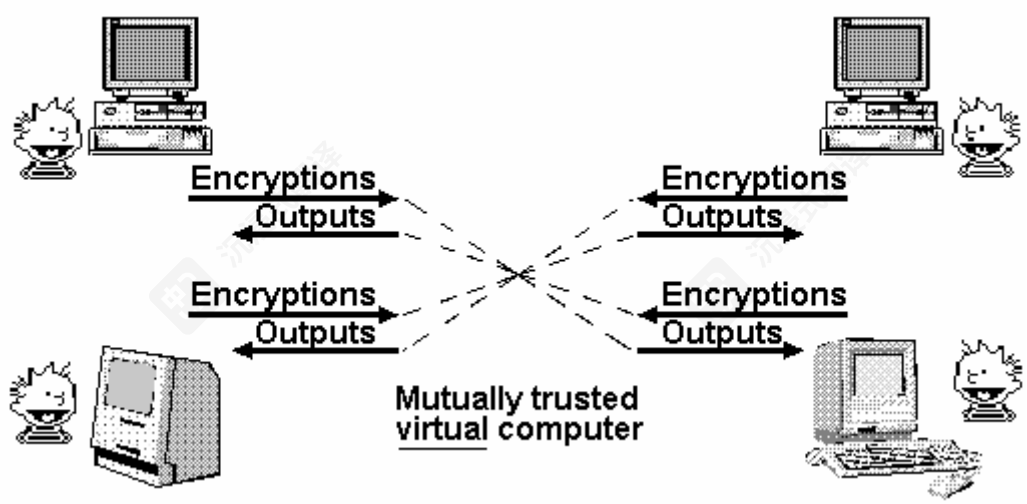

图*2*： 去中心化虚拟信任模型。来自（Szabo，1997）

在去中心化信任模型中，节点不依赖于单一可信方。相反，每个节点加密并独立验证结果，通过网络间的相互验证建立信任。这种设置更符合Qubic的架构，因为它分配了信任，并允许节点在没有中心化监督的情况下达成共识。

Qubic的方案：基于共识的Qubic通过使Computors在共识中集体工作，增强了去中心化模型，实现了高效且可扩展的全局共识，同时保持了去中心化。

2.2.2拜占庭容错（BFT）

在像 Qubic 这样的去中心化网络中，实现拜占庭容错（BFT）至关重要，因为节点可能会失败或行为恶意。通过结合 BFT 原理与基于多数的共识，Qubic 确保了网络在挑战性条件下的韧性。

Qubic 模型中的 BFT 机制：

1. 容错阈值：

   为了维护 BFT，Qubic´ 的模型容忍最多 $f \leq \frac{N-1}{3}$ 个有故障的 Computors 在一个由 N 个 Computors（Lamport 等人，1982）组成的网络中。有了 $N = 676$，这意味着网络可以容忍最多 225 个有故障的 Computors。

2. 冗余计算：

   Qubic 通过让多个 Computors 独立执行相同的计算任务来实现冗余计算。通过汇总这些结果，网络可以识别并忽略异常或恶意数据，依靠多数一致来决定正确结果。

3. 共识投票和协议：

   当 quorum 内至少 $Q \geq 2f + 1$ 个 Computors 对结果达成一致时，即可达成共识。此阈值确保即使存在高达 $f$aulty Computors，共识结果也是可靠的。Qubic 中使用的拜占庭协议要求同意的 Computors 数量大于或等于 451，表示为：

$$Number\ of\ agreeing\ Computors \geq \frac{2N}{3}$$

   此机制确保即使在部分网络故障的情况下也能达成共识，与已建立的 BFT 原则（Castro & Liskov，1999）一致。

4. 故障检测机制：

   Qubic 的系统架构包括可以替换被认为有故障的 Computors 的仲裁者，确保 quorum 操作的可靠性和连续性。此过程允许网络通过无缝替换检测到错误或不一致时的 Computors 来维护完整性，而不会在未来选择中降低单个节点的优先级。此过程通过减少有故障或恶意 Computors 的影响来加强 quorum 系统（Narayanan 等人，2016）。

2.2.3 网络中的角色

Qubic 的治理模式依赖于定义好的角色，每个角色都为支持网络的去中心化运营贡献独特的职责和专业知识。

1. 计算器：

Computors 负责验证交易、执行智能合约、保护网络，并参与共识机制中的多数派共识。每个 Computor 独立运行以执行计算并验证结果，作为共识机制的一部分。

Qubic中计算器的主要方面：

- 可扩展性和灵活性：单个物理节点可以托管多个计算器，增强计算能力并支持网络内的可扩展性。

- 参与陪审团：计算器独立执行任务并对结果进行投票，以形成共识陪审团。这确保了网络内的分布式决策过程。

- 对UPoW的贡献：计算器验证矿工提供的解决方案，以确认它们符合预期标准。此验证过程是集成UPoW到网络运营的关键部分。

- 激励：计算器根据其性能和对网络的贡献获得奖励。QUBIC代币激励其持续高效的贡献，使其目标与网络的计算和共识需求相一致，从而促进稳定性和生产力。

2. 矿工：

矿工为有用的工作量证明模型提供必要的计算能力，专注于训练AI模型和其他对网络AGI目标至关重要的计算密集型任务。

Qubic中矿工的关键方面：

- 计算解决方案的贡献：矿工在有用的工作量证明（UPoW）框架内生成有效解决方案。这些解决方案随后由计算器验证，以确保它们满足在Aigarth中使用所需的条件。

- 激励对齐：矿工根据他们提交的有效解决方案的质量和数量获得奖励。他们的奖励间接与

他们支持的Computors的性能挂钩，加强了网络内的协作和对齐。

- 与Computors合作：通过与高性能Computors协同努力，矿工可以最大化他们的潜在收益，有效贡献于网络的整体计算输出和稳定性。

- 专注于有意义的工作：Qubic鼓励矿工参与直接贡献于网络效用的计算任务，而不是为了安全而执行任意哈希。这些任务涉及与有用工作量证明模型对齐的工作负载处理，支持生态系统内的有意义应用

3. 仲裁人：

仲裁人在Qubic生态系统中扮演着关键的治理和安全角色，监督基于多数同意的共识机制稳定性和完整性。

仲裁人的主要职责：

- 争议解决：仲裁者介入Computors之间的冲突或操作故障。如果一个Computor表现不佳或未能达到操作标准，仲裁者可以将其替换为表现更好的候选者以维持最佳网络性能。

- BFT维护：仲裁者确保网络的一致性故障容错性得到维护，监督系统能够承受最多三分之一Computors恶意行为而不影响安全性。

- 防范中心化风险：治理模型包括制衡机制，其中仲裁者可以被多数Computors（676中的451票）推翻。这种机制保护网络免受仲裁者潜在恶意行为的影响，体现了Qubic对去中心化和安全性的承诺。

3

SYSTEM ARCHITECTURE

本节深入探讨了Qubic的系统架构，旨在构建一个高效、高性能的区块链网络，优化速度、可扩展性和先进AI集成。详细介绍了Qubic网络基础设施的核心组件，包括裸金属部署和节点通信机制，以说明每个组件如何贡献于Qubic的独特能力。每个设计决策背后的理由以及可衡量的改进成果都得到了强调，为Qubic的方法奠定了坚实的技术基础。这些基础设施决策支撑了Qubic的基于共识的仲裁机制和有用工作量证明（UPoW）机制——分别参见第3.2节和第3.1.1节——

支持一个安全且去中心化的网络。

3.1 网络基础设施

Qubic的基础设施旨在满足区块链交易和AI训练的计算需求。下一节将探讨直接硬件操作和优化通信如何提升网络的效率和安全性。

3.1.1 裸金属部署

背景和问题识别

传统的区块链网络通常依赖软件层操作系统（OS）来管理节点基础设施。这种架构会导致延迟并降低硬件效率，尤其是在高交易负载下。硬件与应用程序之间的额外层可能成为性能瓶颈或增加安全管理复杂性（Cachin & Vukolić, 2017）。

为什么选择裸金属部署?

Qubic 通过将其核心软件运行在裸金属硬件上，而不是依赖虚拟机或传统操作系统，从而提升了性能和安全性。这一架构决策消除了操作系统层面的抽象，因此直接利用硬件能力来满足区块链操作、通信协议、智能合约执行和交易处理所需的高性能。

裸金属部署的优势：

- 可靠性：使用 UEFI shell 进行基本功能提供了简化的受控环境，从而减少了与复杂操作系统相关的潜在攻击向量。通过消除对第三方软件平台的依赖，Qubic 提高了可靠性，并减少了意外更新或兼容性问题可能导致的潜在中断。

- 效果：缺乏传统操作系统减少了计算开销和延迟，使 Qubic 能够高效利用硬件功能。UEFI 壳促进了更快的启动时间和简化的硬件级访问，这对于需要高吞吐量的应用至关重要，包括实时处理交易。

- 安全性：通过最小化软件堆栈，Qubic 显著减少了潜在的攻击面，为操作系统级漏洞攻击提供了强有力的防护。裸金属部署方法通过消除通常在互联网上被攻击的漏洞，进一步降低了远程攻击的风险。要攻破裸金属系统，需要物理访问硬件，这对远程攻击者来说是一个显著更困难的任务。这符合 Shostack (2014) 的原则，即减少复杂性并移除不必要的系统层是减少漏洞的关键。

> 此外，设置和维护裸金属节点所需的努力构成了一个自然的进入壁垒，确保只有对系统有深刻理解的坚定参与者才能成为网络的一部分。这有助于构建一个更安全、更具弹性的生态系统。

支持研究和引用

分布式系统和高性能计算领域的研究表明，裸金属部署可以提升系统响应能力并减少关键应用的延迟，特别是在实时环境中（Rosenblum & Garfinkel, 2011）。在一个处理大量交易负载的去中心化网络场景中，例如区块链平台所面临的场景，裸金属架构能够显著提升吞吐量并减少延迟（Cachin & Vukolić, 2017）。

量化指标和性能提升

对Qubic裸金属基础设施的测试，其优化了智能合约执行环境（参见第3.2节），显示出了显著的性能提升：根据智能合约基准测试结果（Qubic Team, 2024），交易延迟减少，吞吐量提升允许每秒进行高达5500万QUBIC币的转账。

3.1.2 节点通信

背景和发现的问题

在任何去中心化网络中，节点之间的通信对于维护共识、数据完整性和及时的交易处理至关重要。传统区块链

通常由于通信协议效率低下而出现瓶颈，导致交易时间变慢和可扩展性降低（Decker & Wattenhofer, 2013）。网络延迟和带宽限制可能会阻碍共识机制，影响整体网络性能。

优化节点通信

Qubic 通过实现一种基于自定义传输控制协议 (TCP) 的通信协议来解决这些挑战，该协议针对低延迟和高吞吐量进行了优化。此协议确保了网络中快速的消息传输，促进了交易和共识相关数据的有效传播。

基于多数投票的共识模型 - 见第 3.2.1 节 - 使多数 Computors 能够快速达成一致，从而最大限度地减少交易最终性的延迟，并提高网络对节点故障的弹性。Qubic 经过设计，旨在优化通信协议和共识机制，以实现网络的更好可扩展性和可靠性。

通信协议的见解

有效的通信协议对于提高交易速度和增强分布式网络中的系统可靠性至关重要。关键研究，如 Nguyen 等人 (2016) 和 Decker & Wattenhofer (2013) 所进行的研究，已注意到在高性能计算环境中，定制 TCP 实现对于减少延迟和增强吞吐量的重要性。

量化指标与性能提升

Qubic 的通信协议使节点能够在亚秒级间隔内达成共识。这一改进使 Qubic 能够处理高频交易，这对需要实时应用程序和服务至关重要，这些应用程序和服务要求立即完成交易。

对等共享

对等节点，即网络中的物理节点，在对等节点共享的上下文中通过IPv4地址进行标识。它们在源代码中被称为“公共对等节点”。每个节点需要一个已知的公共对等节点的初始集合（理想情况下至少有4个）。自己的IP地址应作为普通对等节点包含在knownPublicPeers中。

对等节点可以具有已验证或未验证的状态。一个已验证的对等节点会与其他对等节点共享。knownPublicPeers中的IP地址默认具有已验证状态。

通过 ExchangePublicPeers 消息共享节点，该消息可视为 Qubic 节点的握手。该消息在建立新连接后（节点连接到随机选择的公共节点）发送。共享的 IP 地址会从已验证的节点 IP 地址中随机选择（但是，ExchangePublicPeers 消息中可能会有重复的 IP 地址）。如果节点列表中没有已验证的节点，则必须使用 "0.0.0.0" 作为与 ExchangePublicPeers 消息一起发送的 IP 地址。

如果与已验证节点的出站连接被拒绝，该节点将失去已验证状态。如果与未验证节点的出站连接被拒绝，该节点将从节点列表中移除。如果与未验证节点的出站连接被接受并且收到了 ExchangePublicPeers 消息，该节点将获得已验证状态。如果在通信过程中任何时候检测到协议违规（允许假设远程端运行的是其他东西，而不是 Qubic 节点），即使该节点已验证，也会将其移除。只有当节点列表在移除后仍至少有 10 个条目并且该节点不在初始 knownPublicPeers 中时，才会从节点列表中移除该 IP 地址。

3.2 智能合约执行

为了实现一个能够与高级人工智能应用集成的高性能区块链网络，Qubic采用了一种优化的智能合约执行环境。本节介绍了执行环境以及保护网络完整性同时保持合约隔离所必需的安全措施。

3.2.1 执行环境

背景和识别出的问题

传统区块链上的智能合约在执行速度、灵活性和效率方面常常面临限制，尤其是在处理复杂、高容量的交易时。虚拟机（VM）限制和燃料费会限制可扩展性并阻碍可用性，正如以太坊等平台所显示的那样。基于虚拟机的执行环境带来的开销会导致延迟增加和吞吐量降低。

优化的执行环境

Qubic通过在机器代码级别设计执行环境克服了这些限制，其C++ 功能的一个子集被直接编译成原生代码。不受虚拟机和中间抽象层的限制，Qubic实现了更高的执行速度、减少的计算开销和效率提升。

此环境对 Qubic 至关重要，因为它支持一个需要极高计算能力的 AI 和去中心化应用生态系统。更复杂的计算和实时处理，通过智能合约的原生代码直接执行来实现，是未来集成 AI 功能的要求。

3.2.2 安全措施

背景和已识别的问题

随着智能合约复杂性的增加，其在去中心化网络上的执行相关的安全风险也随之增加。恶意合约利用、跨合约漏洞和隔离不足等问题可能导致网络不稳定，对用户有害（Atzei 等人，2017 年）。执行环境必须确保安全性和完整性，以提供对网络的信任。

安全措施

为应对这些风险，Qubic采用严格的合约验证和隔离策略，旨在确保每个合约的安全独立运行。隔离方法防止未经授权的交互，减少合约间的交叉依赖，降低一个合约对其他合约产生不利影响的风险。

为隔离合约，对其他合约和核心内部函数和数据的访问只能通过精心设计的编程接口（QPI）进行。此外，QPI是开发合约的唯一外部依赖，即禁止使用库。此外，合约不能使用 C++ 已知会带来安全风险的特性，例如指针、低级数组（缺乏边界检查）和预处理指令。合约也永远不会访问未初始化的内存。

每个合同都必须按照以下步骤进行验证：

1. 使用专门的软件工具验证合同，确保其符合上述正式要求，例如不使用禁止的 C++ 功能。

2. 合同的功能必须使用 Qubic 核心中的 GoogleTest 框架实现的自动化测试进行广泛测试。

3. 合同和测试代码必须至少由一位 Qubic 核心开发者审查，以确保其符合高标准。

4. 在将合同完全集成到 Qubic 核心后，合同的功能必须在具有多个节点的测试网络中进行测试，以证明合同在实际中运行良好。

经过此验证过程后，合同可以集成到 Qubic 核心代码的正式版本中。

定量指标和预期收益

创建强大的隔离和验证措施预计将大幅降低潜在安全风险。根据合约隔离的行业标准技术，此类措施可以减少安全漏洞高达95%（Atzei等人，2017年）。凭借先进的安全技术，Qubic为用户提供安全资产，并确保网络操作的完整性，支持其实现安全、高频合约执行的目标。

Qubic在网络基础设施中的架构和智能合约的执行实现了速度、安全性和可扩展性。Qubic通过使用裸金属部署、优化的节点通信和安全的执行模型来解决问题传统区块链问题，从而在去中心化基础设施中设定了新标准

3.3 生态系统

Qubic促进创新和广泛采用的愿景是通过建立强大的生态系统来实现的。Qubic确保其基础设施支持现实世界的用例和持续增长。

3.3.1 产品开发

与行业合作伙伴（如Hashwallet）的合作，专注于开发工具以增强Qubic网络的可用性和安全性。例如，硬件钱包集成旨在提供QUBIC币的安全管理，同时促进

支付系统兼容性。这些合作伙伴关系支持开发关键工具，以提升网络的功能和采用率。

开发团队与社区倡议

Qubic 与 Vottun 等组织合作，后者在创建区块链产品和培养开发者社区方面拥有丰富的经验。这种合作强调构建一个对开发者友好的生态系统，以支持 Qubic 平台上各种应用。Vottun Bridge 解决了区块链互操作性的关键挑战，实现了与以太坊和 Arbitrum 的无缝集成，允许跨链资产转移和流动性共享。正如 Nguyen 等人（2019 年）所强调的那样，区块链互操作性是推动采用和解决孤立网络可扩展性限制的基本因素。

生态系统扩展框架

为支持增长和创新，Qubic 将其生态系统扩展围绕两个核心倡议进行结构化：

- 资助计划：该计划专注于帮助开发者创建各种编程语言所需的工具，例如额外的代码库。它还为超出核心技术范围的贡献提供悬赏资金。Xu 等人（2020 年）的研究突出了资助计划在激励开发者贡献和创建可持续区块链生态系统方面的有效性。

- 孵化计划：旨在支持具有长期潜力的项目，该计划为与 Qubic 能力相符的倡议提供导师指导和初始资金。示例领域包括桥梁、人工智能应用以及基于 Qubic 架构构建的去中心化基础设施项目。

这些合作与倡议展示了 Qubic 专注于构建一个稳健的技术基础，以支持多样化的区块链和人工智能应用。

3.4 用例

本节概述了 Qubic 架构带来的实际应用和潜在用例，说明了其设计如何应对特定的行业需求和挑战。

3.4.1 当前用例

去中心化计算能力

Qubic 通过其实用工作量证明模型，将全球计算资源统一到一个去中心化网络中。它可以执行高需求操作，例如训练人工智能，优化全球未充分利用的资源（Nakamoto，2008）。该共识机制基于多数同意，能够高效地执行和验证计算任务

智能合约

Qubic提供的高性能智能合约为实时去中心化应用程序（dApps）提供了一个可靠的平台。这些合约支持多个领域，包括DeFi、供应链管理和游戏，执行安全且可扩展的操作（Yli-Huumo等人，2016年）。

微支付

QUBIC 币支持无费用的微支付，允许在内容变现和物联网通信等领域进行高频交易。这项功能对于需要无缝、零成本交易的应用至关重要。

AI 训练与验证

通过其实用工作量证明（Useful Proof of Work）模型，Qubic 将计算资源用于训练人工神经网络（ANNs）。这种去中心化方法支持人工智能的进步，为机器学习和人工智能的创新做出贡献。

去中心化交易所

QX是Qubic的去中心化交易所，支持无需中介的数字资产安全透明交易。凭借亚秒级最终性，QX为执行、交易服务和存储提供结构化费用，使其适合高频交易（HFT），并增强网络效用。Vottun桥的开发通过实现Qubic、以太坊和Arbitrum之间的跨链交易，提高了QX的互操作性。

4

CONSENSUS MECHANISM

Qubic网络中最关键的因素之一是共识机制，通过该机制，Computors就区块链状态达成一致，并以安全高效的方式处理交易。Qubic采用基于多数同意的共识机制，并使用拜占庭容错（BFT），如第3.2节所述。下一节将给出详细的协议描述和安全

共识机制的分析。

什么是拜占庭容错（BFT）？

拜占庭容错（BFT）是一种安全模型，允许网络在部分节点行为恶意时仍能正常运行。Qubic在其基于多数同意的共识机制中使用了BFT，以增强安全性和可靠性，即使高达三分之一的节点失效或行为恶意也是如此。有关深入解释，请参阅（Lamport等人，1982年）。

4.1 详细协议描述

与依赖计算工作来保护网络的Nakamoto（2008年）工作量证明模型不同，Qubic的共识机制依赖于多数同意选择和Computors之间的投票来最终确定时间戳和交易。这种方法消除了矿工解决密码学难题的需要，而是通过Computors，通过分布式投票和容错机制来保证安全性和弹性。

尽管Qubic依赖于有用的工作量证明（UPoW）来利用矿工的计算能力进行有用的AI任务，但共识机制在技术上独立。UPoW激励矿工为网络的AI相关目标贡献计算能力，而基于多数同意的共识机制则通过达成关于区块链状态的共识来运作。这两者之间的分离使Qubic能够在共识中实现高效率，而无需强制执行通常以PoW为基础的共识模型所具有的计算开销。

本节逐步介绍了 Qubic 的共识算法，包括证明其有效性和鲁棒性的数学模型和证明。

4.1.1 基于多数的共识算法概述

Qubic 的共识机制旨在实现分布式 Computors 之间的协议，同时容忍拜占庭错误。该算法在称为纪元的离散时间周期内运行，在此期间，交易被提出、验证并提交到区块链。在一个纪元内，存在一个连续的共识轮次序列称为 ticks，Computors 独立地验证和执行交易，并对结果达成协议。

关键组件：

- 计算器：与节点相关联的实体，负责验证交易、执行智能合约以及参与共识。

- 计算器索引：每个计算器在每个纪元都有其特定的索引。索引范围从 0 到 675。

- Tick：在共识算法的一轮中需要执行和达成共识的交易集合，包含智能合约、频谱和宇宙的状态摘要以及时间信息，这些信息唯一地标识了该 Tick 在 Tick 序列中的位置。

  频谱和宇宙包含所有关于当前时间点谁拥有多少 QUBIC 币和其他资产的信息。

  注意：在 *Qubic* 的源代码中，一个 *Tick* 是特定计算器的一票。

- Tick 领导者：Tick 领导者是指负责某个 Tick 的计算器。

  通过此公式可以识别出记账领导者，该公式计算其计算器索引：

$$\text{<COMPUTORINDEX>} = \text{<TICKNUMBER>} \% 676$$

- 共识：达到共识所需的计算器子集。在Qubic中，共识由以下组成：

$$Q = 451 \text{ Computors (out of a total of } N = 676)$$

- 纪元：纪元是更宽泛的时间间隔（1周），由多个记账（共识轮次）组成。在每个纪元中，会完成一系列共识轮次，并且可以根据这些轮次的结果来计算性能或奖励。

- TickData：TickData是记账的定义，宣布将被包含到记账中的交易摘要。记账领导者创建TickData，并将TickData提前在网络中传播。

- 仲裁人：一种用于争议解决和维护网络完整性的机制，如第3.2.3节所述。

4.1.2 Qubic的Quorum共识算法

共识过程可以概述如下：

1. 每个Computor都使用一个从0到675的唯一Computor索引初始化。给定tick *T*的tick领导者是索引为 *C* 的Computor，由T模676计算得出，即：

$$C = T \% 676$$

示例：

Tick: 15104383

ComputorIndex: 515

这解析为：

$$C = 15104383 \% 676 = 515$$

2. 账本领导者创建了“TickData”。
它打包了计划交易的标识符、合约费用，并用时间戳、账本编号和纪元对所有内容进行标记。

每笔交易都由其摘要进行标识，该摘要是对交易进行 KangarooTwelve 哈希的结果。

完整的包由账本领导者签名并广播到网络。广播时间由

TICK_TRANSACTIONS_PUBLICATION_OFFSET 定义。此参数控制账本领导者提前多少个账本发送 TickData。

3. 网络中的所有其他 Computors 将接收 TickData 并验证签名。只有当 TickData 由已知的 tick 领导 Computor 签名时才被接受。

如果 TickData 没有及时到达某个 Computor，这个特定的 Computor 将使用它自己的版本，该版本将是“空”（没有 TickData）。

4. 要处理该Tick，计算器需要拥有所有交易的完整数据，这些交易的摘要已经被Tick领导者打包到TickData中。

计算器检查所有交易是否已经本地存储，如果有任何一个或多个缺失，它将请求其他计算器发送这些交易。

计算器只能在本机所有交易都可用的情况下继续。

5. 当 TickData 通过验证时，所有交易都将可用并已验证，然后 Computor 将就 Tick 进行投票。

6. 每个 Computor 都会分别接收到其他 Computor 的投票。一个 Tick 投票包含 Tick 编号、纪元、Computor 索引、时间戳和发送 Computor 的密码学状态。

理想情况下，每个 Computor 都会看到 676 票（包括自己的）。但收到的投票会根据其内容连续分组以应用多数规则。如果至少有 451 票在同一组中一致，就称为对齐状态，Computor 将同意继续。

根据拜占庭容错（BFT）原则，如 Lamport 等人（1982）提出并由 Castro 和 Liskov（1999）后续改进的，网络只能继续 Tick，当至少有 451 个 Computor 拥有相同视图时，达到三分之二多数以维持网络稳定性。

如果超过225个Computors为空tick投票，这意味着其他任何组都不会超过451票。因此，网络将决定跳过该tick，丢弃计划中的交易。(226+ 规则)。

7. 如果至少451个Computors就tick的内容达成一致（共识），则该tick将被处理，执行交易并进入下一个tick。

如果 226 或更多 Computors 为空票投票，则 Computors 将继续进入下一个 tick 而不执行交易。

故障状态

故障状态用于标记执行可疑操作的 Computors。如果 Computor A 从 Computor B 检测到两个不同的 TickData（或 TickVote）版本，它将标记 Computor B 为故障状态。

仲裁员将使用这些信息来潜在地更换有故障的计算器。

How transactions are sent and propagated across the network

Qubic交易不仅限于简单的代币转账；它们还支持智能合约的执行或Computors之间的通信。与其他区块链类似，一个Qubic交易包含多个基本字段：源地址和目标地址，以及转账金额。除了这些标准字段外，Qubic交易还有一个“Tick”字段，用于指定交易被包含在区块中的期望区块高度，以及一个“InputType”字段，用于指定目标智能合约的流程编号。“InputData”字段提供了要提供给指定智能合约流程的输入数据。

一个广播到节点的交易将默认传播到另外六个节点，这是由DISSEMINATION_MULTIPLIER参数配置的。

Manual intervention from operators

尽管投票仅表示 YES/NO 用于下一个 tick，但由于它还包含节点状态摘要，投票可能会分裂成超过 2 个组，因为如果操作员运行自定义代码或由于不兼容的硬件错误，这些摘要可能会不匹配。在不太可能发生这种情况的情况下，如果无法达成共识，Computors 可能需要手动干预以确保 tick 的推进。

4.2 安全分析

本小节考察了共识机制对各种攻击向量的抵抗能力以及它如何确保网络完整性。

4.2.1 对拜占庭错误的抵抗

拜占庭容错：

- 该共识算法设计用于容忍高达：

$$f \leq \frac{N-1}{3}$$

网络中存在有缺陷或恶意的 N Computors。

影响：

- 安全性：网络确保没有两个诚实的 Computors 对同一纪元接受不同的 tick。

- 活性：尽管存在有缺陷的 Computors，网络仍然继续前进。

4.2.2 确保网络完整性

密码学安全

- 交易由发送方签名。

- 共识消息由负责的Computor签名。

- Computor的状态（频谱、宇宙、SC状态）每tick使用KangarooTwelve进行哈希，以确保网络中的对齐和一致性。

共识弹性

- 仲裁大小和阈值：精心选择的仲裁大小和共识阈值在容错性和性能之间取得平衡。

- 计算器多样性：鼓励计算器的广泛分布可以降低中心化风险并提高安全性。

治理保障

- 仲裁机制：仲裁者监督网络操作，并在异常情况下可以介入，例如检测到广泛的恶意活动。

- 超级多数覆盖：仲裁者可以被多数Computors（676中的451人）覆盖，确保控制权保持去中心化。

5

经济模型

5.1. 发射时间表

在审查了 Qubic 的基础设施和共识机制之后，我们现在转向其经济模型，该模型维持着网络并激励持续的参与。

5.1.1. 初始硬币供应量

在 Qubic 网络的最初阶段，为了确保网络的稳定性和可持续的长期增长，设定了固定的总供应量 QUBIC 硬币。最初，设想了一个最大供应量为 1,000 万亿 QUBIC 硬币；然而，这个数字随后减少了 80%，导致修订后的上限为 200 万亿 QUBIC 硬币。这种有意减少与 Qubic 的目标一致，旨在增强稀缺性并缓解通货膨胀。

- 总供应量：QUBIC 硬币的最大供应量为 200 万亿，从原始供应限制改为增加稀缺性并减少通货膨胀。

总量供应信息与持续的排放和燃烧机制分离，这些机制在发布后会调整流通供应。

5.1.2 排放阶段

QUBIC币的排放是精确计划的，以维持网络参与度同时将通胀水平控制在可控范围内。Qubic的排放模型集成了计划排放、燃烧和减半，并由‘供应观察者’——一个实时控制燃烧速率的智能合约支持。

Qubic 的经济模型结合了排放时间表和通缩机制，以维持长期稳定，借鉴了 Narayanan 等人（2016）探讨的受控发行和奖励分配的概念。这种方法确保网络参与者得到适当的激励，同时避免通货膨胀压力（Beiko，2021）。

排放阶段：

1. 引导阶段（第1-2年）：

- 为鼓励早期采用，排放率设定为每周 1 万亿 QUBIC

- 结果：此阶段促进早期参与。

2. 稳定阶段（第3-5年）：

- 从第123个纪元开始，在第3年，每周燃烧部分排放量，初始燃烧率为15%。

- 减半：大约每52个时期有一次减半，由Quorum批准以确保社区共识。在这些减半期间，燃烧的QUBIC比例增加，有效减少流通中的净供应量，而不会降低每周1万亿QUBIC的基准发行率。

- 供应观察器调整：供应观察器调整燃烧速率以保持稳定。例如，在时期123中，每周排放的15%被燃烧，大约有1490亿QUBIC退出流通。

- 结果：通过燃烧减少有效供应，2024年初始减少15%，然后每年减半有效排放率。

- 需要注意的是，Qubic的排放计划并非固定不变。它被设计为动态的，并随着生态系统的演变而发展。供应观察器允许排放量和燃烧率受到智能合约活动和网络状况等实时因素的影响。这有助于在经济和市场变化时保持灵活性。

3. 可持续性阶段（第6年及以后）：

- 最小排放，侧重于燃烧：当燃烧率缓慢超过排放率时，排放量会达到一个最小值，从而导致总供应量净减少。

- 长期稀缺和价值维持：此阶段突出了代币的稀缺性，而Supply Watcher持续监控并调整燃烧率以缓解过度通缩的风险。随着燃烧率的优先级，整体供应减少，从而增加QUBIC的稀缺性。

图*3*显示了排放阶段和减少计划，说明了燃烧后Qubic的有效每周排放量。从这个视觉表示中，可以注意到Qubic的排放计划随着时间的推移呈系统性地减少，确保稀缺性和可持续经济。

关于灵活性: 由于供应观察者会动态调整燃烧速率，这里的排放和燃烧数据是估计值，不是固定值。供应观察者通过解决矿工和Computors对可能波动的奖励的潜在担忧来帮助稳定性。这确保了供应减少是平衡的，并考虑了网络状况。

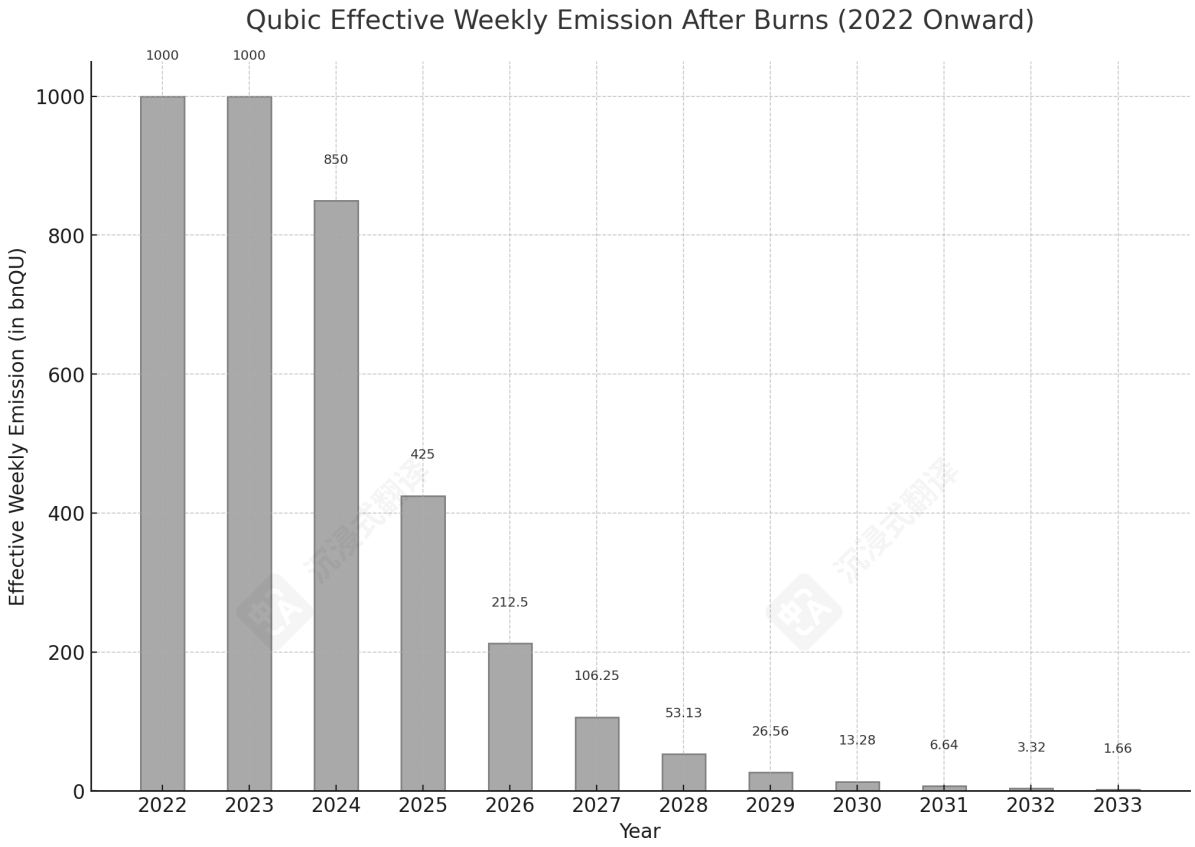

图*3*: *Q*ubic的有效每周排放时间表（燃烧后），展示了多年（从2024年开始）的受控减少，以支持可持续经济

比较说明：Qubic的排放模型受比特币减半策略 (图*4*) 启发，但得益于供应观察者和燃烧机制，它增加了灵活性。虽然比特币通过每四年严格的减半来减少排放，但Qubic允许根据网络当前状态调整燃烧速率。通过这种方式，可以实现受控的稀缺性，并激励网络持续参与，而不会出现固定减半相关的剧烈供应冲击。

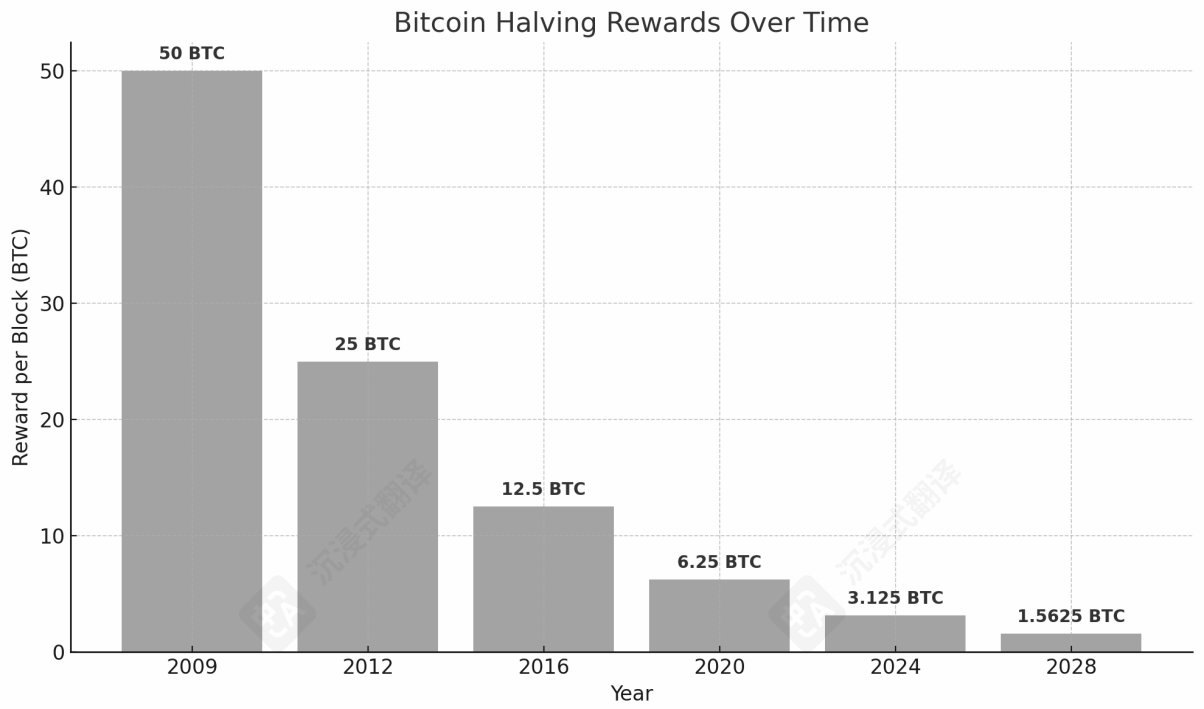

Figure 4: 比特币减半奖励随时间变化

来源： *Independent Reserve,* "比特币减半详解" (Independent Reserve, n.d.)

排放数学模型

● 减半时间表：

$$E(t) = \frac{E_0}{2^{\lfloor \frac{t}{n} \rfloor}}$$

此公式表示一个减半时间表，其中：

- E_0 是初始排放率。
- t 是自减半启动以来的时间。
- n 是排放率减半的时间间隔（以年或时代为单位）。
- $t\ n$ 表示时间 t 时已经发生的减半次数，而 $\lfloor x \rfloor$ 是 x 的向下取整函数（四舍五入到最接近的整数）。

5.1.3 奖励分配

Qubic 的奖励分配机制是一个动态过程。从计算器获得的基准奖励中，他们可以定义特定的捐赠，以支持某些目的。

每个纪元后的收入分配过程如下所示：

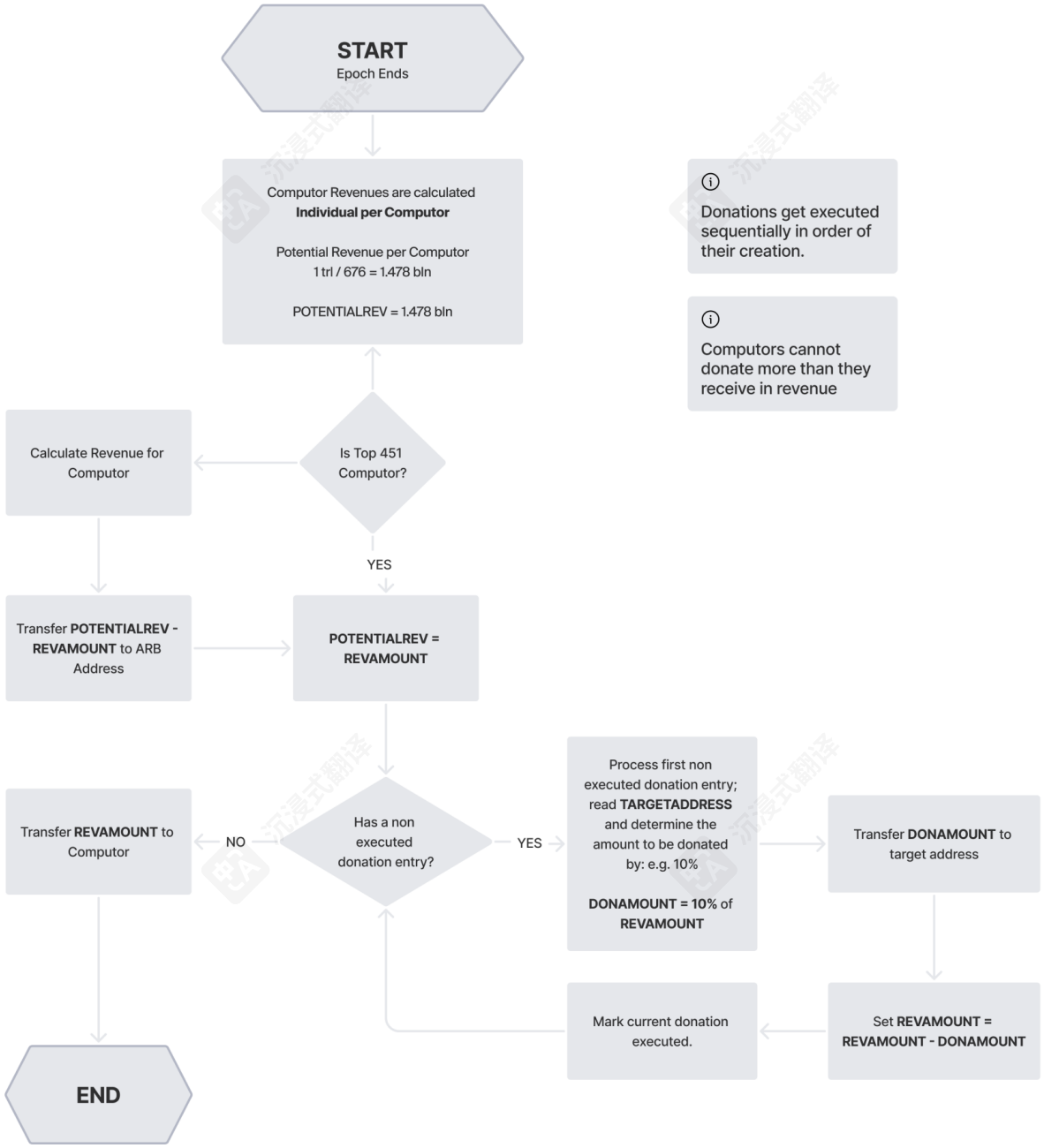

图*5*： 收入计算和分配流程概述

此图表说明了收入如何计算并在网络中分配的整体框架。它从参数的定义开始，例如计算器的基准奖励，并概述了每个纪元后的收入分配过程。

收益分配流程说明：

1. 计算Computors的收益：每个Computor的收益根据其贡献和绩效指标计算。

2. Top 451 Computor检查：只有前451名的Computors才能全额获得奖励，优先奖励高绩效者以激励网络稳定性。

3. 潜在收益调整：如果Computor的绩效低于前451名Computors，其收益将减少，剩余部分将分配给Arbitrator。

4. 捐赠执行：注册的捐赠，如Supply Watcher Burn（15%）和CCF SC（8%），将按顺序从Computor收益中扣除并分配到相应的地址。

5. 最终收入转移：在所有扣除后，剩余收入将转移至 Computor，完成分配过程。

该模型确保收入公平分配，同时支持 Qubic 的更广泛经济目标及捐赠承诺。

图*6* 提供了 Computor 收入计算过程的逐步分解：

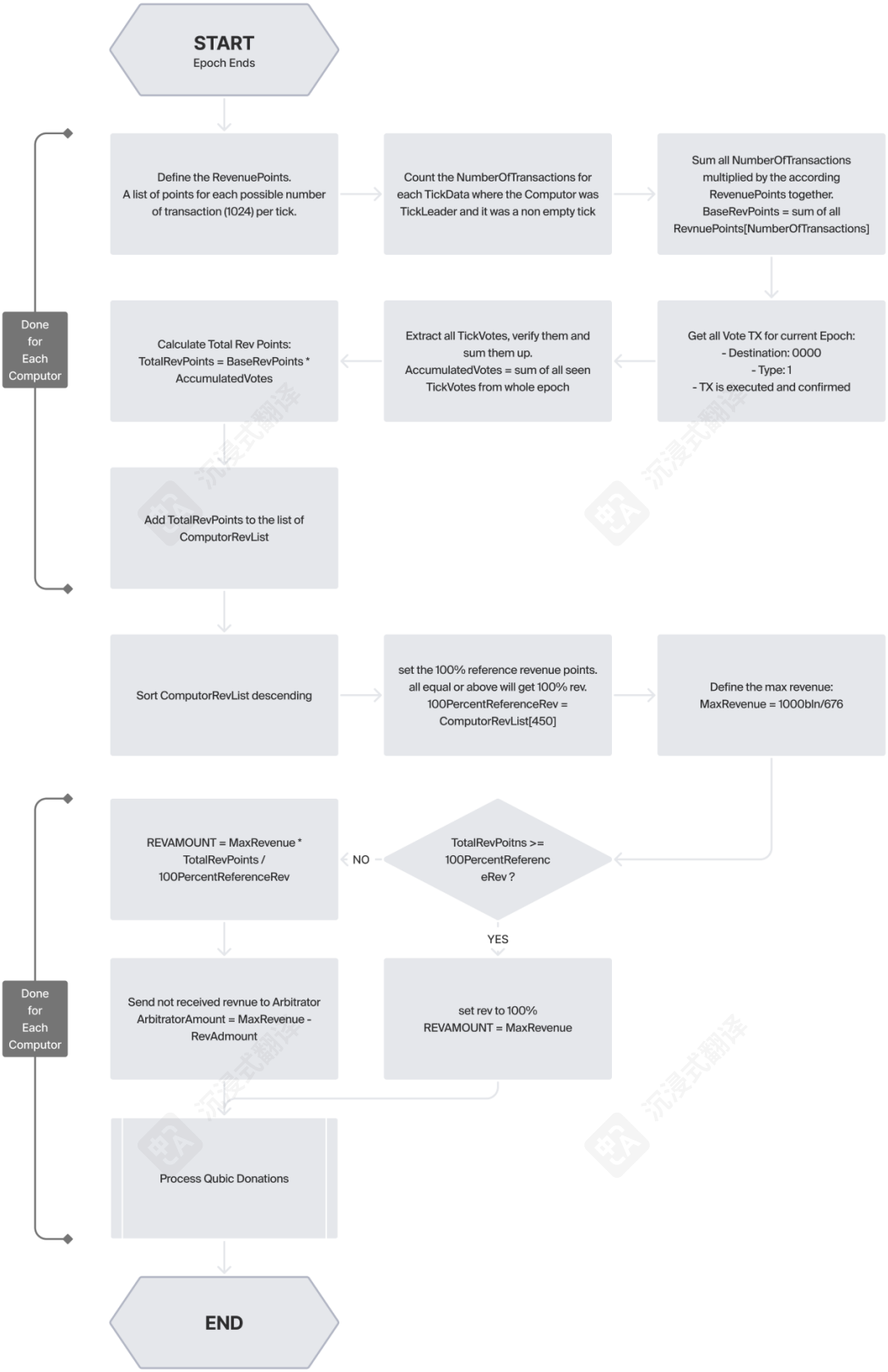

Figure 6: Computor 收入计算详细流程图

- 流程从事件周期的结束开始，之后计算单个Computor的收入。

- Computor前451名检查：该图表显示一个条件步骤，用于确定Computor是否在前451名内。如果不是，将相应地进行收入调整。

- 顺序捐赠执行：捐赠按创建顺序处理，以确保Computor不能捐赠超过其收入的金额。

- 收入转移：最后，在捐赠处理完成后，收入将转移给Computor。

此详细流程加强了Qubic奖励分配的公平性和结构，从而使其与经济目标一致并遵循网络规则。

5.2 通货紧缩机制

通货紧缩机制用于控制 QUBIC 币的流通供应，有助于经济可持续性。

5.2.1 币销毁

币销毁涉及通过发送到不可花费地址来永久移除币，从而使其退出流通。Qubic 采用定期和事件驱动的币销毁。

Qubic 的发行模型包括一个由 Supply Watcher 功能实现的销毁机制。与固定的年度销毁事件或基于交易的销毁不同，Supply Watcher 会实时调整销毁速率。这样，销毁速率会根据网络当前状况进行调整，因此不会引发极端通货紧缩并确保稳定性。

- 周销毁速率：当前的周销毁速率约为 1500 亿 QUBIC。这个数字会根据网络的当前经济状况变化，该状况由 Supply Watcher 监控。

- 供应观察者的作用：供应观察者调整每周QUBIC燃烧的百分比，旨在实现减排与整体网络稳定之间的平衡。该系统为管理有效排放提供了所需的灵活性，允许Qubic适应需求和参与度的变化。

5.2.2 智能合约操作

- 合约执行费用：
    - 执行智能合约产生的费用可能包括销毁成分，进一步减少供应。

5.2.3 对币供应的影响

这些通缩机制的综合效应随着时间的推移减少了流通供应，可能会增加QUBIC币的稀缺性。任何时间点的总供应量由以下公式给出：

$$S_{circulating}(t) = S_{circulating}(t-1) + E(t) - B(t)$$

其中：

- $E(t)$ = 排放在时间t。
- $B(t)$ = 在时间t。总共燃烧的代币

5.3 经济激励

本节探讨了Qubic的经济模型如何就参与和安全对网络中的各方利益相关者进行激励。借鉴第3.1.3节中提出的思想，我们考虑了奖励和经济结构如何支持长期增长和稳定性。

5.3.1 激励的协调

Qubic的经济模型旨在确保参与者因对网络做出积极贡献的行为而受到奖励。

计算器：

- 保持高性能的激励：计算器被激励以可靠和高效地运行以获得奖励。

- 挖矿或参与矿工的激励：当前的 Computors 和潜在的未来 Computors 之间竞争以保持或成为 Computors，需要足够的挖掘解决方案来获得进入下一个纪元的资格。

- 对网络安全性的贡献：通过验证交易和参与共识，Computors 增强了网络的完整性。

矿工：

- 提供计算能力的激励：虽然 Qubic 不会直接奖励矿工，但矿工会通过与关联的 Computors 达成的协议获得奖励，基于他们对 UPoW 任务的贡献，这鼓励他们优化硬件和算法。

- 支持 AGI 开发：矿工的计算工作有助于 Aigarth 内的 AI 训练，使个人激励与网络的更广泛目标保持一致。

代币持有者：

- 供应稀缺性和网络参与度：代币的设计结合了通缩机制来管理供应，而网络扩展旨在创建一个活跃的生态系统。这些要素的结构是为了支持长期可持续性。

- 参与治理：持有代币的用户可能能够参与与其利益与网络成功相一致的治理决策。

5.3.2 奖励的可持续性

Qubic对奖励可持续性的方法得到了Beiko（2021）在排放模型分析中的支持，他在分析中强调了在奖励和网络稳定性之间达到平衡的重要性。Qubic采用受控的排放计划，并结合通缩政策（如代币销毁）来为其利益相关者创造一个稳定且激励的经济环境，这与区块链经济学中的标准最佳实践相一致。根据Beiko（2021）的观点，供应减少需要与参与者的激励相一致，以实现网络的长期健康和参与。

Qubic的经济模型确保奖励在长期内是可持续的：

- 受控排放：排放计划逐渐减少代币发行，防止过度通胀。

- 通货紧缩性抵消：代币销毁抵消通胀压力，平衡供需动态。

- 经济均衡：排放与销毁之间的平衡旨在实现支持网络运营的均衡状态。

5.3.3 网络增长与稳定性

通过激励关键行为，经济模型促进了网络的增长与稳定性。

鼓励参与：

- 多样化生态系统：广泛的Computors和矿工基础增强了去中心化和韧性。

增强安全性：

- 激励合规：奖励激励参与者遵守协议规则。
- 抵御攻击：对恶意行为的经济性惩罚减少了攻击的可能性。

5.3.4 长期经济可行性

经济模型旨在确保Qubic网络的长期可行性。

- 适应性：已建立机制以根据网络状况调整经济参数，从而在应对变化时保持灵活性。
- 与网络目标一致：经济激励与网络目标紧密相连，例如通过Aigarth支持AGI开发。
- 社区参与：通过协调参与者的利益，该模型创建了一个对网络成功高度投入的社区。

6

安全注意事项

Qubic网络的设计和运行中，安全性至关重要。本节深入探讨了支撑网络安全性的密码学基础，并分析了潜在的攻击向量以及为缓解这些攻击而采用的策略。通过利用强大的密码学算法并实施全面的安全协议，Qubic旨在为去中心化交易和计算提供一个安全的环境，包括通过Aigarth进行的与AGI开发相关的那些交易和计算。

6.1 密码学基础

Qubic 网络的安全性依赖于成熟的密码学算法和协议。本小节详细介绍了用于确保数据完整性、真实性、机密性和不可否认性的密码学原语和机制。

6.1.1 密码学哈希函数

算法使用：KangarooTwelve

目的：KangarooTwelve 用于网络内的哈希操作，包括 tick 投票、tick 数据、交易以及频谱、宇宙和智能合约状态的默克尔树。它是 Keccak 算法家族（SHA-3 基于此）的一个变体，但针对速度和可扩展性进行了优化。KangarooTwelve 的可扩展性和速度使其非常适合高吞吐量环境，正如 Bertoni 等人（2018 年）所强调的那样。其碰撞抵抗能力和效率支持 Qubic 对实时共识的需求，同时确保网络内数据的完整性。

属性：

- 抗碰撞性：在计算上不可行地找到两个不同的输入产生相同的哈希输出。
- 抗原像性：给定一个哈希输出，在计算上不可行地找到产生该哈希的输入。
- 抗二次原像性：给定一个输入及其哈希，在不可行地找到具有相同哈希的不同输入。

在Qubic中的作用：

- Tick哈希：通过预定义的一组密钥的哈希将每个tick链接到前一个tick，确保tick的完整性，使用KangarooTwelve进行高效计算。
- 确保 Computor 状态的一致性：通过计算频谱、宇宙和智能合约状态并包含它们在共识协议中，Computors 确保它们在每个 tick 中的状态一致。

- 识别交易：使用 KangarooTwelve 计算每个交易（也称为摘要）的哈希值，用于识别交易。

- Merkle Trees: 用于高效且安全地计算大型数据结构的哈希值，例如频谱和宇宙。

6.1.2 数字签名

使用的算法：FourQ（改编版）

FourQ是由微软研究院开发的一种椭圆曲线。它专为密钥协商方案（椭圆曲线Diffie–Hellman）和数字签名（Schnorr）而设计，并提供约128位的 безопасности (Costello & Longa, 2015)。

- 目的：Sign/Verify用于验证网络内的交易和消息，确保只有授权方才能发起操作。

- 属性：

    o 真实性：验证发送者的身份。

    o 不可否认性：防止发送者否认其签名的真实性。

    o 完整性：确保消息未被篡改。

- 在Qubic中的作用：

    o 交易签名：用户使用私钥对交易进行签名，Computors使用相应的公钥验证签名。

    o 共识消息：计算器在共识过程中对其投票和提案进行签名，以保持问责制和可追溯性。

6.1.3 密钥管理

公钥和私钥：

- 生成：密钥使用安全的随机数生成器生成，以确保不可预测性。

- 存储：用户必须安全地存储私钥。Qubic鼓励使用硬件钱包或安全可信环境来存储密钥。

6.1.4 安全通信协议

消息签名：

- 目的：确保真实性和完整性

- 实现：在Qubic中发送的消息由发送者签名。这使得接收者能够验证消息的真实性和完整性。

6.2 攻击向量与缓解措施

本小节识别了Qubic网络中的潜在漏洞，并概述了用于缓解这些漏洞的策略。通过主动应对这些威胁，Qubic增强了其抵御恶意行为者和网络中断的韧性。

在缓解潜在的Sybil和51%攻击方面，Qubic的模型结合了拜占庭容错原则，并从Simmons等人（2009年）审查的网络攻击防御分类研究中汲取灵感。

6.2.1 Sybil攻击

- 描述：攻击者创建多个身份（Sybil节点）以获得不成比例的影响力。

- 缓解措施：

    o 有用的工作量证明（UPoW）：UPoW将计算能力导向有用任务，如AI训练，使攻击成本对任何集结必要计算资源以成功执行Sybil攻击的攻击者都变得不划算。

    o 正式签名：在Qubic中，只有676个computors有投票权。没有相应的密钥，因此不可能进行Sybil攻击。

6.2.2. 分叉攻击

- 描述：恶意Computors创建替代链来混淆或分裂网络。

- 缓解措施：

  o 强最终性：一旦一个区块被共识机制接受，它就被认为是最终的，后续的区块在此基础上构建。

  o 链选择规则：诚实的计算者会遵循由共识机制投票累计支持度最高的链。

6.2.3 串通攻击

- 描述：一组恶意Computors串通一气，操纵共识决策。

- 缓解措施：

  o 容错阈值：只要参与串通的Computors数量少于226，该算法就能容忍串通行为。

  o 随机化仲裁人选择：对每个仲裁人进行不可预测的选择，降低了持续串通的可能性。

6.2.4 重放攻击

- 描述：攻击者重发有效交易，以破坏网络。
- 缓解：

  o 忽略重复：已知的交易被计算器忽略。

6.2.5 51%攻击

威胁描述：

- 攻击者控制了网络超过50%的计算资源或投票权，允许他们通过撤销交易或阻止新交易确认来操纵区块链。

缓解策略：

- 拜占庭容错：共识机制容忍高达 1_3 个有故障的 Computors，这使得攻击者在未控制网络重要部分的情况下难以成功。

- Computors 的去中心化：鼓励广泛参与可降低中心化风险。

- 在 Qubic 中，要接管网络，需要 `>= 451` 个投票，约占总网络的 2/3。

- 经济性威慑：执行 51% 攻击所需资源的成本超过了潜在收益。

参考： (Eyal & Sirer, 2014)

6.2.6 日食攻击

威胁描述：

- 攻击者通过控制所有节点的入站和出站连接来隔离一个节点或一组节点，使攻击者能够操纵受害者对网络的看法。

缓解策略：

- 多样化对等选择：节点与一组多样化的对等节点保持连接，减少所有连接被攻击者控制的可能性。

- 连接限制：限制单个IP地址或子网的连接数量。

- 分离入站和出站连接：节点不能被阻止出站连接。

- 周期性对等体刷新：定期随机更新对等体连接，以防止长期隔离。

6.2.7 智能合约漏洞

威胁描述：

- 智能合约代码中的缺陷可能导致意外行为、安全漏洞或被攻击者利用。

缓解策略：

- 代码审计：在部署前由可信第三方对智能合约进行强制审计。

- 限制语言功能：防止在智能合约中使用复杂或风险较高的语言功能。

6.2.8 量子计算威胁

威胁描述：

- 量子计算的兴起可能会打破传统的加密算法，从而危及网络的安全。

缓解策略：

- 抗量子密码学：

    o 研究与开发：监控量子计算领域的进展，并开发抗量子密码方案。

    o 算法灵活性：设计协议以允许在新的密码算法可用时进行集成。

- 后量子算法：探索如基于格的密码学（例如，NTRU）或基于哈希的签名（例如，XMSS）等算法。

参考：(Bernstein 等人，2017)

6.2.9 恶意软件和节点被攻破

威胁描述：

- 恶意软件感染或未经授权的访问可能会损害节点，导致数据泄露或参与恶意活动。

缓解策略：

- 安全软件实践：实施代码安全最佳实践和定期安全评估。
- 隔离技术：Qubic 在裸金属上运行，无需底层操作系统。
- 定期更新和补丁：保持软件和依赖项更新以减轻已知漏洞。

7

结论

7.1 贡献总结

本白皮书概述了 Qubic 的架构及其在区块链和人工智能 (AI) 领域内克服挑战的方法。通过使用第一层区块链，Qubic 集成了经济机制，例如有用工作量证明 (UPoW) 和拜占庭容错 (BFT) 基于共识的机制，将网络安全与生产性 AI 计算相结合。通过 Aigarth，Qubic 支持可扩展的 AGI 开发，通过创建更资源高效和道德去中心化的平台，使其区别于传统的区块链解决方案。该设计还通过包括受控排放计划和通货紧缩措施的经济模型解决了经济可持续性问题，平衡奖励分配并促进长期参与。

Qubic 的基础设施展示了性能改进，例如亚秒级交易最终性和裸金属部署，这减少了延迟并增加了计算能力。这些功能使网络能够支持高需求、实时应用程序，同时保持能源效率。此外，Qubic 的治理模型通过在网络参与者之间分配决策权来促进去中心化和弹性，并在不利条件下确保容错能力。

8

参考文献

8.1. 参考文献列表

1. Atzei, N., Bartoletti, M., & Cimoli, T. (2017). 对以太坊智能合约的攻击调查 *(SoK)*. 第*6*届国际安全与信任原理会议 *(POST 2017)* 会议录, 计算机科学论文集, 10204, 164– 186. Springer. https://doi.org/10.1007/978-3-662-54455-6_8

2. Beiko, T. (2021). 以太坊 *EIP-1559:* 交易费市场. 以太坊改进提案. https://eips.ethereum.org/EIPS/eip-1559

3. Belchior, R., Vasconcelos, A., Guerreiro, S., & Correia, M. (2021). 区块链互操作性调查：过去、现在和未来趋势. ACM 计算机调查, 54(8), 文章 168. https://dl.acm.org/doi/10.1145/3471140

4. Bernstein, D. J., 等 (2017). 后量子密码学：现状.年度国际密码学会议 (CRYPTO). https://eprint.iacr.org/2017/314

5. Bertoni, G., Daemen, J., Hoffert, M., & Van Assche, G. (2018). KangarooTwelve：基于 Keccak-p 的快速哈希算法. 来自 https://keccak.team/files/KangarooTwelve.pdf

6. BitCompliance S.L. (2024). *Qubic* 代币法律性质的合法性声明.来自 2024 年 7 月 19 日发布的法律文件.

7. Cachin, C., & Vukolić, M. (2017). 现实世界中的区块链共识协议. arXiv 预印本 arXiv:1707.01873. https://arxiv.org/abs/1707.01873

8. Castro, M., & Liskov, B. (1999). 实用拜占庭容错. https://pmg.csail.mit.edu/papers/osdi99.pdf

9. Costello, C., & Longa, P. (2015). *FourQ: Q*曲线上梅森素数的四维分解. 在 ASIACRYPT 2015上展示。微软研究院。从 https://www.microsoft.com/en-us/research/project/fourqlib/ 获取。

10. Decker, C., & Wattenhofer, R. (2013). 比特币网络中的信息传播. IEEE P2P 2013会议论文集, 1–10。 https://ieeexplore.ieee.org/document/6688704

11. Eyal, I., & Sirer, E. G. (2014). 多数并不足够：比特币挖矿易受攻击。
金融密码学与数据安全。https://arxiv.org/abs/1311.0243

12. Gabuthy, Y. (2023). 基于区块链的争议解决：见解与挑战。
游戏，14(3)，34。https://doi.org/10.3390/g14030034

13. Independent Reserve。 (n.d.)。 比特币减半解释。 Independent Reserve。
检索到 [检索到 11月 3, 2024],
https://www.independentreserve.com/blog/knowledge-base/bitcoin-halving
解释

14. Lamport, L., Shostak, R., & Pease, M. (1982). 拜占庭将军问题
https://lamport.azurewebsites.net/pubs/byz.pdf

15. 中本聪，S. (2008). 比特币：一个点对点的电子现金系统.
https://bitcoin.org/bitcoin.pdf.

16. Narayanan, A., Bonneau, J., Felten, E., Miller, A., & Goldfeder, S. (2016). 比特币和
加密货币技术：综合介绍。普林斯顿大学出版社
https://press.princeton.edu/books/hardcover/9780691171692/bitcoin-and-
cryptocurrency-technologies

17. Nguyen, T. A. N., Gangadhar, S., & Sterbenz, J. P. G. (2016). 性能评估
数据中心网络中*TCP*拥塞控制算法的研究。会议录
第11届未来互联网技术国际会议（CFI '16），21–28。
https://doi.org/10.1145/2935663.2935669

18. 阮氏·T·T·K，阮氏·H·T·T，& 阮氏·N·H. (2019). 区块链中博弈论应用综述
区块链中博弈论. 来自 https://arxiv.org/pdf/1902.10865.pdf.

19. Qubic团队（2024年）.*Qubic*实现每秒超过*5500*万次转移，用于
智能合约执行。 博客文章。
https://qubic.org/blog-detail/qubic-achieves-over-55-million-transfers-per-
second-for-smart-contract-executions

20. Rosenblum, M., & Garfinkel, T. (2005)。 虚拟机监视器：当前
技术和未来趋势。 IEEE Internet Computing, 38(5), 39–47。
https://ieeexplore.ieee.org/document/1430630

21. Shostack, A. (2014). 威胁建模：为安全而设计. Wiley Publishing. https://www.wiley.com/en-us/Threat+Modeling%3A+Designing+for+Security-p- 9781118809990

22. Szabo, N. (1997). 在公共网络上形式化与安全化关系 https://nakamotoinstitute.org/formalizing-securing-relationships

23. Xu, J., Lu, Q., Gao, F., & Zhang, H. (2020). 激励区块链生态系统发展：博弈论方法. Journal of Systems Science and Complexity, 33(4), 918–933. https://link.springer.com/article/10.1007/s11424-020- 9189-2

24. Yli-Huumo, J., Ko, D., Choi, S., Park, S., & Smolander, K. (2016). 区块链技术当前研究现状？——系统综述. PLoS ONE, 11(10), e0163477. https://journals.plos.org/plosone/article?id=10.1371/journal.pone.0163477

25. Zolfagharinejad, M., Alegre-Ibarra, U., Chen, T., et al. (2024). 脑启发计算系统：系统文献综述. 欧洲物理杂志 B, 97, 70. https://doi.org/10.1140/epjb/s10051-024-00703-6

8.2. 进一步阅读

为了支持对白皮书中概述的核心技术和方法的深入探索，以下资源提供了关于区块链基础知识、共识机制、密码学、经济模型和高级人工智能 (AI) 集成方面的见解。

区块链架构和共识机制

- Nakamoto, S. (2008). *Bitcoin: A Peer-to-Peer Electronic Cash System.* 这篇开创性论文介绍了去中心化数字货币的概念，为工作量证明等区块链共识模型奠定了基础。

- Lamport, L., Shostak, R., & Pease, M. (1982). *The Byzantine Generals Problem.* ACMTransactions on Programming Languages and Systems, 4(3), 382–401*A*经典著作，介绍了拜占庭容错（*BFT*），对于理解分布式网络中的共识及其在*Qubic*共识模型中的实现至关重要。

- Narayanan, A., Bonneau, J., Felten, E., Miller, A., & Goldfeder, S. (2016). Bitcoin and Cryptocurrency Technologies: A Comprehensive Introduction. Princeton University Press.

  区块链技术的深入介绍及其背后的密码学原理，包括对共识和交易验证的讨论。

- Castro, M., & Liskov, B. (1999). 实用拜占庭容错。操作系统设计与实现第三次会议论文集。拜占庭容错（*BFT*）模型的概述，对于理解去中心化网络中的共识至关重要。

密码学基础和安全协议

- NIST (2015). *SHA-3*标准：基于置换的哈希和可扩展输出函数。 NIST FIPS 202。
  SHA-3 的详细规范，这对于区块链安全至关重要
  协议，包括用于区块头和 *Merkle* 树的哈希函数。

- Bertoni, G., Daemen, J., Hoffert, M., & Van Assche, G. (2018). *KangarooTwelve:* 基于 *Keccak-p* 的快速哈希 提交给 NIST 的 SHA-3 派生函数。*KangarooTwelve* 是一种基于 *Keccak-p* 构建的实用哈希函数，提供快速、安全的哈希功能，适用于高吞吐量应用，支持 *Qubic* 的加密安全需求。

- Micali, S., Rabin, M. O., & Vadhan, S. P. (1999). 可验证随机函数。
  第 40 届计算机基础理论研讨会论文集
  科学。
  可验证随机函数（*VRFs*）的介绍，它是实现公平且
  不可预测的共识选择的关键组成部分。

智能合约和可编程货币

- Szabo, N. (1997). 在公共网络上形式化和保护关系。 第一星期一，2(9)。
  一本关于智能合约的基础性著作，详细阐述了可编程货币和自动执行协议的概念，这些概念是去中心化应用的核心。

- Luu, L., Chu, D. H., Olickel, H., Saxena, P., & Hobor, A. (2016). *Making Smart Contracts Smarter.* ACM SIGSAC Conference on Computer and CommunicationsSecurity.对智能合约漏洞的批判性探索，包括用于防止常见安全漏洞的形式化验证方法。

区块链中的代币经济学和经济模型

- Kroll, J. A., Davey, I. C., & Felten, E. W. (2013). 比特币挖矿经济学，或存在对手方的比特币。 WEIS.探讨了挖矿中的经济动态和激励结构，与理解*Qubic*的发行模型和奖励机制相关。

- Saleh, F. (2021). 无浪费的区块链：权益证明。 金融研究评论，34(3)，1156–1190。分析了权益证明（*PoS*）及其相对于工作量证明（*PoW*）的效率，其概念适用于*Qubic*的可持续经济模型。

高级人工智能集成和AGI发展

- Silver, D., Huang, A., Maddison, C. J., Guez, A., Sifre, L., & Van Den Driessche, G.(2016). 使用深度神经网络和树搜索掌握围棋游戏。 自然，529(7587)，484-489。一篇里程碑式的论文，展示了高级人工智能在复杂决策中的实际应用，与理解*AGI*在*Qubic*中的作用相关。

- Gabriel, I. (2020). 人工智能、价值观与对齐。伦理与信息技术，22(1), 11-21。doi:10.1007/s10676-020-09578-0。探讨了人工智能发展的伦理挑战，特别关注人工智能价值观与社会目标的对齐。

- *Vivancos, D. (2023).* 艺术学。*https://www.linkedin.com/pulse/artificiology-david-vivancos-5zmqf/.* 一篇关于人工智能、通用人工智能和人类认知增强交叉点的发人深省的观点。注意：本文未经同行评审，反映了作者的个人见解。

博弈论与分布式系统

- Yao, A. C. (1982). 安全计算协议。第23届计算机科学基础会议论文集 (SFCS)。安全计算的理论分析，为去中心化系统的安全性和稳定性奠定基础。

- Eyal, I., & Sirer, E. G. (2014). 多数并不足够：比特币挖矿易受攻击。国际金融密码学与数据安全会议。分析了*51%*攻击的脆弱性及缓解策略，为*Qubic*的*BFT*增强共识模型提供了适用见解。

9

附录

9.1 术语表

本文件中使用的专业术语和缩写的定义。

1. **AGI (通用人工智能)**: 人工智能系统理解、学习和应用智能以处理广泛任务的能力，相当于人类认知能力。

2. **Aigarth**: 一个与 Qubic 深度集成的项目，利用实用工作量证明 (UPoW) 模型训练 AGI 模型和其他高级人工智能应用。

3. **裸金属部署**: 直接在硬件上运行应用程序，无需操作系统或虚拟化，以提高性能和安全性。

4. **燃烧机制**: 一种永久从流通中移除代币的过程，通常通过智能合约执行费用等网络活动实现，以帮助控制通货膨胀。

5. **拜占庭容错 (BFT)**: 一种安全模型，即使在部分节点行为恶意的情况下也能使网络功能正常。

6. **Computor**: Qubic网络中的一种专用节点，负责验证交易、保障网络安全，并通过参与共识机制获得QUBIC币作为奖励。

7. **经济学**: 支配网络中币的发行、分配和用途的经济结构和原则，在此例中是指Qubic网络中的QUBIC币。

8. **发行模型**: 将QUBIC币投入流通的有序时间表，指导奖励如何以及何时分配给参与者。

9. **Epoch**: Qubic网络中的一个预定义时间周期（一周），用于结构化奖励分配、挖矿资格和共识活动的阶段。

10. **效率因子 (E)**: 表示矿工在所有尝试中成功解决方案比例的乘数，反映了硬件和算法的效率。

11. **Hash Rate**: 计算能力的衡量标准，以每秒迭代次数（it/s）表示，指示矿工硬件可以尝试的潜在解决方案数量。

12. **Miners**: 在有用工作量证明（UPoW）模型中提供计算能力以支持任务的网络参与者，因 Computors 的有效贡献而获得 QUBIC 币作为奖励。

13. **QUBIC coins**: Qubic 网络中使用的数字货币，用于奖励 Computors、促进交易和支持网络操作。

14. **Qubic Network**: 一种去中心化平台，设计用于安全、可扩展和高效的计算，通过有用工作量证明（UPoW）模型支持 AGI 开发、经济和共识。

15. **Quorum**: 一种需要多数阈值的共识模型，通过拜占庭容错确保网络完整性。

16. **Reward Allocation**: QUBIC 币按网络参与者对网络的贡献比例进行分配的过程。

17. **解决方案提交率 (S_{rate})**: 有效计算解决方案提交到网络的比率。

18. **频谱**: 存储每个实体在当前时间/tick拥有的QUBIC硬币数量，包括一些关于进出转账的信息。

19. **供应监视器**: 一个监视QUBIC硬币总供应量的Qubic网络实体，通过触发销毁事件来维持经济稳定。

20. **Tick**: 共识算法中待执行和同意的交易集合，包含智能合约、频谱以及宇宙的整体状态摘要和时间信息，这些信息唯一地标识了序列中的Tick。

宇宙以及时间信息，它唯一地标识了序列中的该时间点。

21. **宇宙**: 存储有关 Qubic 区块链中当前时间 / tick 存在的所有资产（不包括 QUBIC 币）的信息，包括谁拥有和拥有它们的信息。

22. **有用的工作量证明 (UPoW)**: 将计算工作导向人工智能和其他有价值任务，而不是传统 PoW 模型中典型的任意问题解决。

白皮书贡献者致谢

这份白皮书代表了一项协作努力，来自区块链技术、密码学、人工智能和经济建模领域的专家做出了贡献。以下个人在其研究、起草和审查中发挥了关键作用：

Daniel Diez, iam333 , Zgirt, JOETOM, Dr Philipp Werner, dkat, frog-rabbit, mksala, pjdubs, Oreo, Eric Fung, David Vivancos, Dr Jose Sanchez, Come-from-Beyond, Foleycious, Talentnodes, Peter, MrUnhappyX, Dr Karin Lorez, CryptoDeighs, Crypdro

Qubic社区的见解和贡献也同样表示衷心感谢。