下一个ICP？详解去中心化计算机Quilibrium

撰文：Lydia Wu

读者应知悉：由于 Quilibrium 的主网尚未发布，且目前的公开信息较少，本文中关于激励机制、经济模型、融资历史、路线图等的描述仅立足于当下的时间点，实际情况在未来可能发生改变。本文的写作主要出于研究与科普目的，请勿作为投资参考，同时也欢迎同业的批评探讨。

### 1. 报告要点

#### 1.1 核心投资逻辑

#### 1.2 主要风险

#### 1.3 估值

由于 Quilibrium 尚处于非常早期的阶段，我们暂时无法得出项目的准确估值。但从流通市值和全流通市值来看，相比概念有重合度的其他市场玩家，Quilibrium 目前的市值具备一定的吸引力。

### 2.业务分析

Quilibrium 自己定位为「去中心化的互联网层协议，提供云计算的便利而不牺牲隐私或可扩展性」，以及「去中心化的PaaS解决方案」。针对这一定位，本部分将围绕以下几个问题对 Quilibrium 的业务进行阐述。



#### 2.1 业务定位

2.1.1 从计算谈起

无论在 Web2 还是 Web3， 「计算」都是一个至关重要的概念，是应用开发、执行和扩展的动力来源。

在传统互联网架构中，计算任务通常由中心化的服务器完成。云计算的出现提高了计算的可扩展性、可访问性和成本效率，并逐渐取代传统计算成为主流。

从服务内容看，大型云服务商提供的云服务模型通常可以分为基础设施即服务 (IaaS) , 平台即服务 (PaaS) 和软件即服务 (SaaS) 三大类，分别对应不同需求和能力的主体，提供对资源的不同级别的控制能力。一般终端用户比较熟悉的是 SaaS。PaaS 和 IaaS 主要面向开发人员。





在以太坊等主流区块链中，计算通常由去中心化节点完成。这种方式不依赖中央控制的服务器，每个节点在本地执行计算任务，并通过共识机制确保数据的正确和一致，但去中心化计算的能力和处理速度通常无法与传统云服务相比。

而 Quilibrium 试图在传统互联网的计算能力和可扩展性，以及区块链的去中心化之间找到一个「平衡」，为应用开发开辟新的可能。



2.1.2 计算机系统的中心化问题

对于大部分终端用户来说，计算机的中心化问题并不易于感知。这是因为终端用户直接面对的大多是硬件层面的计算机系统。我们的 PC、手机等设备分散在世界各地，并在个人控制下独立运行。这种分布式的物理存在使得计算机系统在硬件层面不一定中心化。

与相对分散的硬件形成对比的是，现有的计算机系统在网络架构和云计算服务层面明显更加中心化——亚马逊 AWS, 微软 Azure, Google Cloud 在 2024 年一季度的云服务市场份额超过 67%，与后来者拉开了显著的差距。



并且，作为 AI 浪潮「卖水人」，云服务商强者恒强的趋势似乎还在延续。微软 Azure 作为 OpenAI 的独家云服务提供商，近一年来的业绩增速一改往日颓势，呈现出加速增长的态势。在微软 2024 财年第三财季（即 2024 自然年一季度）财报中，Azure 和其他云服务的收入增长了 31%，高于市场预期的增长 28.6%。



除了市场竞争层面的考量，中心化的计算机系统带来的隐私和安全问题也愈发得到关注——几家大型云服务商的每一次宕机都会产生大范围的影响。数据显示，从 2010 年至 2019 年间，AWS 累计出现过 22 次突发故障，年均故障次数达 2.4 次。除了亚马逊自身的电商业务受影响之外，使用 AWS 的 Robinhood、迪士尼、Netflix、任天堂等公司的网络服务也大规模中断。

2.1.3 去中心化计算机的提出

在此背景之下，去中心化计算机的必要性被反复提出。由于近年来中心化云服务商越来越多地采用分布式架构，通过在多个地点复制数据和服务来避免单点故障，以及通过边缘存储来提升性能，去中心化计算的叙事重点逐渐转移到数据安全、隐私、可扩展性和成本效益上。

我们首先来辨析几个由不同项目提出来的去中心化计算机的概念，它们的共同特征是希望通过分散数据存储和处理，构建一个全球性的分布式计算平台，支持去中心化应用的开发。

值得注意的是，ICP, AO 和 Quilibrium 都不是传统意义上的区块链。它们不依赖线性的区块排列结构，但保持了区块链的核心原理如去中心化、数据不可篡改等，可以被视为是区块链技术范畴的自然扩展。虽然 ICP 至今未能将其宏图伟业落实，但 AO 和 Quilibrium 的出现确实带来了一种影响 Web3 未来的新可能性。

下表对比了三者的技术特点和应用方向，以期帮助读者理解「Quilibrium 是否会重蹈ICP覆辙」，以及同样作为去中心化计算的前沿解决方案，Quilibrium 和被称为「以太坊杀手」的AO有什么区别。



#### 2.2 共识机制

在传统区块链中，共识机制处于一个较为抽象和核心的层面，它定义了网络如何达成一致、如何处理和验证交易以及其他操作。不同的共识机制选择将影响网络的安全性、速度、扩展性和去中心化程度等。

Quilibrium 的共识机制被称为「有意义的工作证明」 (Proof of Meaningful Work/PoMW)，矿工被要求完成对网络有实际意义的工作，比如数据存储、数据检索、网络维护等。PoMW 共识机制的设计整合了如密码学、多方计算、分布式系统、数据库架构和图论等多个领域，旨在降低对单一资源 ( 如能源或者资本 ) 的依赖，确保网络的去中心化程度，以及在网络规模扩大的同时也能保持安全性和扩展性。

激励机制是确保共识机制能够顺利运行的关键。Quilibrium 的激励分配不是静态的，而是会根据网络状态动态调整，以保障激励与需求相匹配。Quilibrium 还引入了多重证明机制，允许一个节点验证多个数据片段，在节点和核心资源不足时依然可以维持网络运行。

我们可以用一个简化的公式来理解矿工的最终收益，其中单位奖励会根据网络规模动态调整。

收益=评分×单位奖励

评分的计算基于多种因素，具体公式如下：



其中，各个参数定义如下：

以上四个参数的加权总和将会有一个主题上限 (TC)，作用是将该数值限制在一定范围内，从而避免某些参数过大导致的评分不公



Quilibrium 目前在运行的节点数已经超过 6 万，实际运行中的节点收益可能会根据每个版本之间参数权重的不同而有所波动。在 v1.4.19 版本以后，矿工收益可以实时查看，但需要等主网上线后才可以领取。

#### 2.3 网络架构

Quilibrium 的核心业务是去中心化的 PaaS 解决方案，其网络架构主要由通信、存储、数据查询和管理、操作系统构成。本节将重点介绍其设计方案相对于目前主流区块链的不同之处，对技术细节和实现方式感兴趣的读者可以查阅官方文档和白皮书。

2.3.1 通信

作为网络的基础建构， Quilibrium 的通信由四部分构成。

a.密钥生成

Quilibrium 提出了一种基于图论的 PCAS (Planted Clique Addressing Scheme) 密钥生成方式。和传统区块链技术相似，PCAS 也使用了非对称加密——每个用户拥有一个公钥和一个私钥，公钥可以公开，用于加密信息或验证签名；私钥则保密，用于解密信息或生成签名。两者的区别主要在于密钥的生成方式、表现形式以及应用方向上（见下表）。



b.端到端加密

端到端加密 (E2EE) 是确保节点之间通信安全的关键组件，只有通信双方可以看到明文数据，即使是帮助传递信息的系统或中介也无法读取信息内容。

Quilibrium 采用了一种名为 Triple-Ratchet 的端到端加密方法，相比传统的 ECDH 方案提供了更高的安全性。具体来说，传统方案通常使用单一的静态密钥，或定期更新密钥，而Triple-Ratchet 协议会在每次通信后都更新密钥，从而实现前向保密、泄露后保密、可否任性、重播保护、无序消息传递等功能。这种方案特别适合群组通信，但相对而言复杂性和计算成本也较高。

c. 混合网路由

混合网络 (Mixnets) 是一个黑盒子，可以接收发送者的信息，并将它们传递给接收者，而外部攻击者即使能访问到黑盒子外的信息，也无法将发送者和接收者关联起来。

Quilibrium 采用了 RPM (Random Permutation Matrix) 技术，提供了一个在结构上复杂且难以被外部及内部攻击者破解的混合网络架构，在匿名性、安全性和可扩展性方面具有优势。

d.点对点通信

GossipSub 是一种基于发布 / 订阅模型的点对点消息传递协议，在区块链技术和去中心化应用 (DApps) 中应用广泛。 Quilibrium 的 BlossomSub 协议是对传统 GossipSub 协议的一个扩展和改进，目的是提高隐私保护，增强抵抗 Sybil 攻击的能力，并优化网络性能。

2.3.2 存储

大多数传统区块链使用加密哈希函数作为基本的数据完整性验证工具，并依赖于共识机制来确保网络一致性，这样的机制有两个主要的局限性：

通常不包括对存储时间的验证，对于抵御基于时间或计算能力的攻击没有直接的机制

存储和共识机制通常较为分离，可能导致数据同步和一致性上的问题

Quilibrium 的存储方案使用了可验证延迟函数 (VDF) 设计，创建了一个时间依赖性的链式结构，并集成了存储和共识机制。结合下图，可以总结出这种方案的几个特点：

输入处理：通过使用如 SHA256 和 SHAKE128 等哈希函数处理输入，任何数据的微小变化都会导致哈希值的显著不同，从而使数据更难被篡改、更易于验证

延迟保证：计算过程被故意设置为耗时的。计算任务必须按顺序执行，每一步都依赖于前一步的结果，无法通过增加计算资源来加速进程，以确保输出是基于连续和确定时间的计算得到的。由于生成过程无法并行化，任何试图重新计算或更改已经公布的 VDF 结果的行为都需要相当长的时间，这为网络参与者提供了足够的时间来检测和响应

快速验证：验证一个 VDF 结果所需的时间远少于生成这个结果所需的时间，通常只需要对最终结果进行一些数学检验或者利用一些辅助数据来确认结果的有效性



这种基于时间证明的链式结构不依赖传统区块链中块的生成，理论上可以减少 MEV 攻击和抢跑现象。

2.3.3 数据查询和管理

传统区块链大多使用简单的键值存储或 Merkle Tree 来管理数据，这种结构在表达复杂关系和支持高级查询方面通常较为受限。并且目前大多数区块链系统在节点执行查询时不提供内置的隐私保护机制，这也是零知识证明等隐私增强技术提出的背景。

Quilibrium 提出了一种「无记名超图」 (Oblivious Hypergraph) 构架，结合了超图结构和无记名转移 (Oblivious Transfer) 技术，可以在保持数据隐私性的同时支持复杂的查询能力。具体来说：

超图结构：允许边连接多个顶点，增强了表达复杂关系的能力。这种结构可以直接映射多种数据库模型，使得任何类型的数据关系都可以在超图上表达和查询

无记名转移技术：即使是处理数据的节点也无法了解正在访问的具体数据内容，增强了数据查询过程中的隐私保护

2.3.4 操作系统

操作系统并不是一个区块链原生的概念。大多数传统区块链主要关注共识机制和数据的不变性，通常不提供复杂的操作系统级别功能。比如以太坊虽然支持智能合约，但其操作系统功能相对简单，主要限于交易处理和状态管理。

Quilibrium 设计了一种基于其超图数据库的操作系统，并实现了常见的操作系统原语，例如文件系统、调度器、类似 IPC 的机制、消息队列、控制键管理等，这种直接在数据库上构建操作系统的设计可以为开发复杂的去中心化应用提供支持。



#### 2.4 编程语言

Quilibrium 的开发使用 Go 作为主要编程语言，也结合了 Rust 和 JavaScript。Go 语言的优势在于其处理并发任务的能力、简洁的语法以及活跃的开发者社区。根据 Tiobe 发布的编程语言排行榜，Go 语言近年来的排名上升明显，在最新的 6 月榜单中已经位列第 7 名。同样使用了 Go 语言做底层开发的区块链项目还有以太坊、 Polygon 和 Cosmos。





### 3.项目情况

#### 3.1 项目历史和路线图

Quilibrium 的白皮书发布于 2022 年 12 月，其路线图大致分为 3 个阶段：Dusk, Equinox 和 Event Horizon。

Quilibrium 目前仍处于非常早期的阶段，团队以两周为单位进行网络的更新迭代，目前的最新版本为 v1.4.20。由于团队删除了路线图的 1.5 阶段，网络的 1.4 版本之后将直接升级到 2.0 版本。2.0 版本也即主网，是 Dusk 阶段的结尾，预计将在七月下旬正式推出，届时将允许 $QUIL 的桥接。

根据暂定计划，Equinox 和 Event Horizon 阶段将为流媒体、AI/ML 模型训练等更高级的应用提供支持。

#### 3.2 团队和融资

Quilibrium 的创始人 / CEO 是 Cassie Heart。在创立 Quilibrium 之前，她是 Coinbase 的高级软件工程师，在软件开发和区块链领域拥有超过 12 年的经验。

由于 Cassie 对中心化的社交媒体平台持反对态度，她本人以及 Quilibrium 的项目账号主要活跃于 Farcaster。Cassie 的 Farcaster 账号拥有超过 31 万关注，其中包括以太坊创始人 Vitalik。Cassie 同时也是 Farcaster 的开发者。

从 Quilibrium 的开发者数据面板上看，Quilibrium 项目的开发自 2023 年 4 月开始，随后一直稳定进行。显示的开发者共有 24 位，主力是 Cassie Heart (Cassandra Heart)。





Quilibrium 的团队尚未公开其融资历史和投资机构。

#### 3.3 通证模型分析

$QUIL 是 Quilibrium 的原生代币，采用 100% 公平发射的形式，所有代币产出均来自节点运行。团队本身运营一小部分节点，但拥有的代币占比不到 1%。

$QUIL 没有固定的通证模型，代币总供应无上限，但是会根据网络采用的速度动态调整——网络规模增加时，会相应释放更多的代币作为节点激励；若规模增长放缓，相应的代币释放速度也会降低。

下表是团队和社区成员对代币释放时间表做出的预测，目前的流通量为 3.4 亿 ，预计最终供应量将收敛于 20 亿左右，具体的释放情况还需视生态发展而定。



#### 3.4 风险

Quilibrium 现阶段潜在的风险点包括：

项目处于非常早期的阶段，主网尚未发布，且项目复杂度较高，技术可行性和市场需求的验证尚未完成

短期内可能会面临来自知名度更高的 Arweave AO 在用户心智和开发者方面的竞争

没有固定的通证模型，代币释放速率可能不稳定，对于投资者来说增加了一定风险

### 4. 估值

类公链的基础设施估值本身就是一个非常复杂的过程，涉及 TVL、链上活跃地址、dAPP 数量、开发者社区等多个维度，而 Quilibrium 尚处于非常早期的阶段，Arweave AO 的代币 $AO 也尚未开放交易，因此我们暂时无法得出项目的准确估值。

我们在此列出与 Quilibrium 具有一定概念重合度的项目流通市值和全流通市值（数据截至 2024 年 6 月 23 日 )，供大家参考。



5. 参考内容与致谢本文的写作需要感谢海哥 (@PleaseCallMeWhy)、蓝哥和 Connor 的审阅和意见。

https://quilibrium.com/quilibrium.pdf

https://paragraph.xyz/@quilibrium.com

https://dashboard.quilibrium.com/

https://www.youtube.com/watch?v=Ye677-FkgXE&ab\_channel=CassandraHeart

https://dune.com/cincauhangus/quilibrium

https://source.quilibrium.com/quilibrium/ceremonyclient/-/graphs/main?ref\_type=heads

https://www.tiobe.com/tiobe-index/

https://www.blocmates.com/meal-deal-research-reports/quilibrium-crypto-not-blockchain-long-live-the-internet

https://www.statista.com/chart/18819/worldwide-market-share-of-leading-cloud-infrastructure-service-providers/

https://s2-labs.com/admin-tutorials/cloud-service-models/

https://medium.com/@permadao/%E5%8E%BB%E4%B8%AD%E5%BF%83%E5%8C%96%E4%BA%91%E6%9C%8D%E5%8A%A1%E8%BF%9B%E5%8C%96%E5%8F%B2-%E4%BB%8E-dfinity-ic-%E5%88%B0-arweave-ao-839b09b4f3ff

https://www.microsoft.com/en-us/investor/earnings/FY-2024-Q3/press-release-webcasthttps://x.com/perma\_daoCN/status/1798565157435830416

https://x.com/Pow2wer/status/1802455254065402106