



Menlo One

satoshi@menlo.one | www.menlo.one

Menlo One

扩大去中心化应用规模的框架

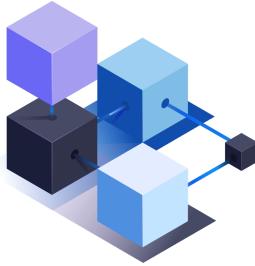
白皮书

Matthew Nolan

白皮书版本 : 5.0.1

2018 年 8 月 1 日





Menlo One

扩大去中心化应用规模的框架

白皮书

摘要

使命

非投资要约

我们致力于解决的商业问题

降低 dApp 构建成本

使去中心化应用对于用户像基于云端一样快速

改善 dApp 的用户体验

dApp 用户和开发人员的成本

Menlo One 潜在使用场景

证券代币和其他金融产品市场

点对点共享经济网站

下一代 ICO 市场

原创内容和媒体

用户生成的内容可为创作优质内容的用户带来回报

希望迁移到 Web 3.0 的传统 Web 模式

潜在使用场景的简要列表

我们是谁，我们为什么创立 Menlo One？

法律考虑因素

Menlo One 组成部分

Menlo 代币——我们软件的基石

将 ONE 用作获取数据的货币

将 ONE 用作获取关注的货币

将 ONE 用作良性激励机制

促进代币驱动型经济的代币驱动数据库

声誉证明

先付出后获取的代币激励政策

代币登记节点背景

Menlo TownHall——通信层

在线聊天

HashMail：私人付费消息服务

不可篡改性

声誉

TownHall 内的代币经济

TownHall 框架

TownHallJS 应用程序

身份验证与用户数据

数据模型

核心功能

主要部件

用户旅程 1：创建新消息

用户旅程 2：在留言板上给消息点赞

用户旅程 3：兑换发布话题所获的 ONE

Menlo Guild——治理层

设计考虑因素

押注声誉的代币登记节点

用于筛选搜索结果的质量信号使用

Guild 系统架构

Menlo Pocketbook ——交易层

Menlo 智能钱包

预授权交易

自动买入

跨链互操作性

KYC 身份管理

_Toc521081766

Menlo Core——数据层

系统架构考虑因素

关键术语

身份认证

关注度经济

使用以太坊验证存储于 IPFS 的数据

区块链存储动态内容的解决方案

通过缓存内容节点提升以太坊性能

声誉证明激励

激励后的内容节点网络

用于资料查看的 Granter 智能合约

检索证明

使用激励型 Validator 缓解攻击向量

系统架构组成部分

Menlo 客户端应用

Menlo 节点应用

智能合约矩阵

代币经济学

系统内的 ONE 流

用户赚取 PoR 的方式

Menlo Core 使用场景

平台开发路线图

早期历史（2016-2017 年）

路线图（2017-2018 年）

路线图（2018-2019 年）

团队

顾问

最重要的增长因素：开发者社区支持

项目治理结构

Menlo 代币发售

代币发售阶段

代币发售奖励结构（主要公开版）

代币发放

参考文献

致谢

了解更多信息

摘要

Menlo One 既是一个框架，也是一组开源工具与协议，可供开发人员打造速度、易用性和成本效益可与中心化应用媲美的去中心化应用。我们的框架采用了包括以太坊网络 [26]、IPFS [25]在内的多种去中心化技术，还可前向兼容其他去中心化网络。我们协同使用这些技术，抵消其弱点并利用其优势，为用户创造可与其在中心化网络养成的习惯形成竞争的体验。我们的去中心化数据库和声誉证明激励体系让下一代市场、社交媒体平台和未来应用成为可能，其速度和性能可媲美其中心化的前身。

Menlo One 提出了三项关键技术：

1. 桌面原生应用程序，运行包括以太坊和 IPFS 在内的网络轻节点，可自动执行预先批准的交易。此应用通过开放端口与网络浏览器中的 dApp 进行通信。
2. 声誉证明算法，其利用代币登记节点设计模式来激励良性贡献并促进网络发展。
3. 去中心化数据库网络，其缓存来自去中心化网络的数据，从而为用户提供与传统 Web 应用相媲美的速度和体验，同时带来分布式区块链与身俱来的安全保证。

本文描述了三种类型的参与者：

1. **卖方**：Menlo One 是一门关注度经济。卖方是寻求他人关注，以便出售或推广产品、服务或品牌的个人或公司。卖方持有希望获得关注物品的资料。卖方可能包括餐馆，它希望在参观点评网站上吸引饥肠辘辘的顾客，可能是正在招聘的公司，它希望在求职网站上获得潜在应聘者的关注，也可能是想要在二手车网站上出售车辆的个人。
2. **内容节点**：提供应用从 IPFS 和以太坊提取数据，包括：卖方资料及云托管高性能计算机数据库中的缓存。
3. **用户**：收费查看卖方资料者。款项来自卖方列表智能合约。

代币经济学简要概述

根据比特币和以太坊的精神，用户必须做出一定的支付来支持网络。由于网络上的大多数使用场景都涉及吸引某人关注并开展销售，因此这种模式存在问题，因为要潜在顾客交钱来参观你的展厅并不是理想模式。要解决这一问题，应当完全由卖方来支持生态系统。卖方将 Menlo 代币打入智能合约，支付给内容节点，以便快速向用户提供他们的资料或产品页面。Menlo 代币用于支付数据、服务和关注费用。

注意：要探索我们框架内的所有功能，ICO（首次代币发行）市场就是一个很好的使用场景，因为整个行业已经上链。我们在本文中经常提及 ICO 市场，不过我们框架内当然也有许多其他使用场景。

使命

Menlo One 的使命在于消除价值交换的中间环节，我们正在开发各种工具，让去中心化应用程序易于使用、便宜且快速，使其能够与中心化的前辈们竞争，从而大规模刺激人们采用去中心化应用程序。促进世界更加繁荣平等。作为该领域的第一个框架，它将助力于促成我们所希望的）为区块链社区创建去中心化应用程序所需的催化剂，让应用程序的使用频率可以像 Facebook 或 YouTube 一样。框架一直是几乎每种网络技术快速发展的催化剂。我们认为 Menlo One 可以做到同样的事情。

非投资要约

本文档概述我们对产品的愿景。我们强调致力于解决的问题，以及我们公司为解决这些问题而采取的行动计划。撰写本文档时，我们正计划启动 Menlo 代币 (ONE) 销售，这是 TownHall 软件运作的重要组成部分。购买 ONE 并非对下述产品开发的投资。ONE 作为产品出售，是 TownHall 正常运作的必须环节。我们在本文档中概述了我们的长期产品愿景。



我们致力于解决的商业问题

降低 dApp 构建成本

与其他技术不同，去中心化应用程序的生态系统没有任何允许开发人员实现常用功能的强大框架。通过纳入用于预授权交易的 API，我们的目标是提高构建去中心化应用程序的速度，方式与 Rails 提高在 Ruby 编程语言上构建中心化应用程序速度类似。

使去中心化应用对于用户像基于云端一样快速

去中心化网络的一个固有缺陷是交易速度不及传统的高性能网络堆栈。我们的框架旨在提高来自多个去中心化网络的读写速度，使其与传统的高性能网络堆栈交互速度相当。

改善 dApp 的用户体验

今天以太坊生态系统所利用的许多工具都是在几年前创建的，专门面向具备技术的受众。使用 MetaMask，Parity 和其他 Web 3.0 工具与 dApp 交互令人十分不快，因为即使像点赞帖子一样简单的事，也需要用户批准交易。

dApp 用户和开发人员的成本

在以太坊区块链上交易的成本目前是采用 dApp 的障碍。虽然从比特币继承的理念是所有用户都应该为支持网络而付出一点代价（这是去中心化概念的基础），但事实很简单，要求用户进行交易妨碍了人们接纳主流 dApp。这对于试图销售产品的任何应用程序都是个问题，因为企业无法因为“走进他们的展厅”就向用户收费。我们相信，通过使用可互换代币 (ONE) 抵消以太坊网络固有的瓦斯成本，我们可以克服这一障碍。

Menlo One 潜在使用场景

证券代币和其他金融产品市场

通过非中介化可以使许多金融工具和服务更加高效。例如，股权众筹这一领域需要通过新的法律来规范提供这些证券的平台。某人可以建立一个完全透明的去中心化众筹市场，如 WeFunder 或 AngelList，在这些市场中，没有必要通过监管来确保某些产品不会被推广盖过其他产品。这将包括 ICO、证券代币和其他类型的加密货币交易，甚至是令 OTC 加密货币交易更加安全的完全去中心化系统。我们的框架将让市场的用户体验与亚马逊购物一样友好。

点对点共享经济网站

使用 Menlo One 框架，可以构建完全去中心化的 Airbnb，Uber 或其他共享网站。这些网站占据了相当大比例的交易，而这些交易可以交给卖方和用户。

下一代 ICO 市场

有许多方案可改进现有 ICO 模式 [16]。最值得注意的是由 Vitalik Buterin 提出的 DAICO [17] 和互动币产品 [18]，由 Vlad Zamfir 提出的安全代币销售机制 [19] 以及 Simon de la Rouviere 提出的各种连续代币模型 [20]。其中大部分承诺为投资者提供保护、透明度和去信任化。除标准钱包可使用之外，这些新模式还涉及社交关系和复杂界面。目前尚不清楚哪些模式可能适用于 ICO 市场，但 Menlo One 的功能使其成为支持此类模式的最理想环境，且我们的系统旨在向前兼容这些模式。

原创内容和媒体

近年来，我们看到了 Spotify、Youtube 和其他媒体网站等内容公司的崛起，这些公司在创作者收入以及内容创作者付费机制方面不够透明。Menlo One 提供了一个框架，可以去除中介，让用户和内容创作者享有透明和价值。

用户生成的内容可为创作优质内容的用户带来回报

Web 2.0 建立在中介的基础上，从鼓励用户“免费”分享内容的网站上获得广告，但不会为用户提供同等价值的回报。示例包括：Facebook、Google、Yelp、YouTube 等。Menlo One 可用于构建一个系统，让用户和贡献者可以根据他们提供的价值或内容获得奖励。

希望迁移到 Web 3.0 的传统 Web 模式

我们的框架可用于取代现有的中心化社交媒体网站、电子商务、求职网站、新闻媒体和其他传统模式上的传统网络堆栈。虽然这些系统可以使用 Rails 这样的框架构建，但 Menlo One 却利用区块链技术来使用户能够通过自己的关注获利。利用包括 Visa 在内的传统支付系统对于加密货币中常见的小额交易和微交易而言成本过高。

潜在使用场景的简要列表

- 第一个真正去中心化的 ICO /证券代币/会员代币市场。
 - 有史以来第一个 DAICO 市场和管理系统。
 - 另一个版本的 Yelp，让用户通过撰写餐厅评论而获得报酬，餐厅能够为预先认证的客户提供优惠券。
 - 去中心化的亚马逊或 eBay，不向卖方收取费用。
 - 去中心化的 Airbnb、Uber 或其他分享网站，对卖方更透明，不收取任何费用。
 - 游戏内产品市场。
 - 一个具有小额赏金任务的就业市场。
-
- Stack Overflow 的获利版本，奖励用户解决复杂软件问题。
 - Quora 的变现版本，其奖励高价值贡献者提供专家建议。

- 类似于 Reddit 的在线社区，发布最佳帖子的用户可获得奖励。
- Trello 等风险管理系统促进用户相互竞争完成任务以获付款奖励。
- 在线徽标设计社区，客户设立徽标赏金，最佳徽标可获得报酬。
- 初创公司激励去中心化小组或 **Guild** 评价其产品。

我们是谁，我们为什么创立 Menlo One？

我们是连续创业者和技术专家，在构建面向消费者的成功网络产品方面拥有丰富的经验和理解，自成立以来一直从事区块链领域。使用及开发区块链技术时，我们密切关注其弱点。我们知道需要什么样的产品，我们就要构建它。

法律考虑因素

面向潜在 Menlo 代币购买者的重要注意事项？

任何有意购买 Menlo 代币的人士应阅读并了解下文所述的重要注意事项，然后再购买 Menlo 代币。

开发失败或中止

鉴于技术复杂性和难度可能不确定、不可预见和/或不可克服，开发 Menlo One 协议或协议特定的组件随时会因任何原由（包括资金不足）而失败或中止。根据开发失败或中止可能发生的时间，上述活动会造成无法使用部分或所有 Menlo One 功能，从而对 ONE 的使用造成负面影响。

有限信息披露

Menlo One 的多项技术规格和参数可能会在 ONE 销售前后更新和更改。尽管本白皮书包含有关 Menlo One 和 Menlo, Inc. 的关键信息，但由 Menlo, Inc. 自行决定是否有必要作出任何调整或更新。Menlo, Inc. 无义务就 Menlo One 的开发事宜（包括：进度及里程碑）定期更新白皮书，且无义务及时提供完全访问 Menlo, Inc. 逐步形成的有关 Menlo One 的所有信息。

不断变化的监管环境

ONE 等加密代币正在或可能受到不同司法管辖区监管机构的详细检查。Menlo, Inc. 可不时收到一个或多个监管机构发出的问询、通知、警告、请求或裁决，甚至会下令暂停或切断与 Menlo One 或 ONE 相关的任何操作。因此会严重影响、妨碍或终止 Menlo One 或 ONE 的开发、营销或促销等。鉴于任何司法管辖区的监管政策随时会有变化，Menlo One 和 ONE 在任何司法管辖区内的有利监管局面随时会消失或变化。ONE 不时会被定义为不同司法管辖区内的虚拟商品、数字资产、证券或货币，应当地监管要求会禁止其在特定司法管辖区开展贸易或持有。

Menlo 代币的预期用途；不作为证券营销或销售

相应功能仅限 TownHall 软件内使用，ONE 无意保留软件外的任何使用价值。购买 ONE 不会获得任何所有者权益、投票权、管理权、财产利益、或任何收入或利润共享权益。ONE 的预期用途有激励大家参与 TownHall 生态系统，鼓励用户为生态系统作出积极增值贡献，及支持代币登记节点系统。鉴于大家均未把 Menlo 代币视为证券，Menlo 代币并未依据《1933 年证券法案》或任何州的证券法进行注册销售。既无证券交易委员会，也无任何州的证券监管机构审核过 ONE 销售的条款。尽管我们认为 ONE 并不是证券，但联邦或州证券监管机构可能判定 ONE 销售应遵守相关证券法。ONE 属于证券、应遵守相关证券法等此类判定可能会对 ONE 代币购买者产生负面影响。

加密技术的进步

代码破解等加密技术的进步或量子计算机开发等科技进步会对包括以太坊虚拟机和 Menlo One 在内的所有基于加密技术的系统造成风险。这会造成 ONE 遭窃、丢失、消失、损坏或贬值。可以预测未来加密技术或安全创新会抵消此类技术进步而引发的风险。

开源卖方

Menlo One 是 Menlo, Inc. 发起的开源项目，旨在赢得有意改善代币销售流程信任度、透明度和安全性的社区支持。尽管 Menlo, Inc. 可能对围绕 Menlo One 进行开发的任何社区发挥影响力，但其无法完全控制 Menlo One 的开发、营销或运作等。任何人士均可开发补丁或升级 Menlo One 的源码，无需事前获得任何人士的授权。因此，Menlo One 会受制于不重视 ONE 购买者最大利益的第三方。或许，很少或没有社区会为 Menlo One 进行开发，因而 Menlo One 不会享受到其他开源项目所享有的益处。

源码缺陷

Menlo, Inc. 无法保证 Menlo One 的源码一直不会有缺陷。Menlo One 的源码可能随时会有缺陷、错误和漏洞（统称为“**缺陷**”），用户可能会禁用某些功能、泄露用户信息，或对 Menlo One 造成负面影响。此类缺陷会危害 Menlo One 的使用和/或安全，进而对 ONE 的价值造成不利影响。开源代码依赖于提升社区知名度及代码解决方案的透明度。Menlo, Inc. 应不断与支持 Menlo One 改进、优化和完善源码的社区密切合作，但 Menlo, Inc. 惟无法保证任何此类社区会参与开发，也无法保证 Menlo, Inc. 会解决 Menlo One 源码中已明确的缺陷，从而足以弥补此类缺陷。

源码更新

Menlo, Inc. 和/或使用 Menlo One 的社区会不时更新、修订或修改 Menlo One 的源码。Menlo, Inc. 无法预见或保证任何此类更新、修订或修改能药到病除。因此，任何更新、修订或修改会导致意料之外的结果，从而对 Menlo One 运作或 ONE 使用造成负面影响。

私钥

访问 ONE 所需的私钥丢失或损坏可能是无法逆转的。仅唯一公钥和私钥的所有人能通过本地或在线钱包控制 ONE。购买者负责保护自己钱包中私钥的安全。一旦购买者的此类私钥丢失、遗失、泄露或销毁，无论 Menlo, Inc. 还是任何其他人均无法帮助购买者访问或取回相关的 ONE。

热门程度

ONE 的价值极大取决于 Menlo One 用户采纳率。Menlo One 从未想过 ONE 一经销售就会立即受到追捧、普及或广泛使用。出于各种原因，Menlo One 可能绝不会在美国或其他国家的代币销售社区成为中坚力量。此外，尽管 Menlo, Inc. 出于开发 Menlo One 之目的而推动 ONE 的购买和使用，但投机者会持有大量 ONE，从而人为提高 ONE 价格。用户和商业利用不足可能会造成 ONE 价格波动加剧，进而会危害 Menlo One 的长期发展。

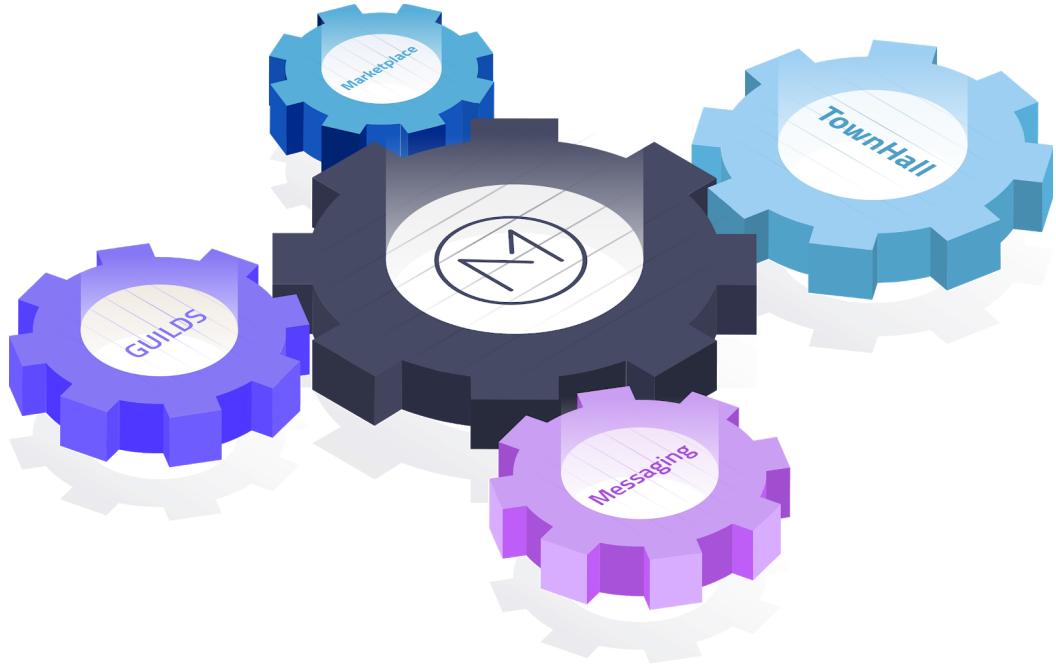
流动性

ONE 并非任何个人、实体、中央银行、或国家、超国家或准国家组织发行的货币，也无任何硬资产或其他信用支持。 ONE 的市场流通和贸易由相关市场参与者协商一致的价值决定。无论 Menlo, Inc., 还是任何其他人员均无义务从购买者或任何其他 ONE 持有者处兑换或购买任何 ONE。 Menlo, Inc. 恕不保证 ONE 的流动性和市场价格。有意出售 ONE 的购买者必须找到一(1)个或多个有意以商定价格购买的买家，整个交易流程昂贵又费时。在任何特定时间，加密货币交易所或其公开市场均不会将 ONE 挂牌上市交易。Menlo, Inc. 不会采取任何措施让 ONE 在任何加密货币交易所或其他交易所挂牌上市。

竞争

Menlo One 是基于无人申索其源码版权的开源计算机软件。因此，任何人可合法复制、设计、修改、升级、改进、重新编码、改编或利用源码和/或 Menlo One 的底层平台，用以开发计算平台或软件。上述情形超出 Menlo, Inc. 控制范围，可能会危害 Menlo One 和 ONE 的使用。此外，有些第三方拥有的资源可能多于 Menlo, Inc., 因此会开发独立、无关联且有竞争力的协议。任何情况下，Menlo, Inc. 均无法消除、预防、限制或尽量减小此类旨在与 Menlo One 竞争的效应。

Menlo One 组成部分



Menlo 代币——我们软件的基石

Menlo 代币 (ONE) 是以太坊公链上的开源代币，其兼容 ERC20 标准 [7]。 ONE 是款举足轻重的软件，旨在与我们的软件完美兼容，可以出售给开发人员，借以打造功能完善的产品。按 ERC20 标准进行设计，便于用户之间在没有中介机构授权的情况下自由转移 ONE，这是我们系统实现完全去中心化的一项关键属性。

将 ONE 用作获取数据的货币

为了确保 Menlo One 能为用户提供与中心化应用程序（如 Facebook 或 YouTube）平常一样快速的响应式体验，Menlo One 上的数据必须由高性能内容节点提供，我们设想在 AWS 托管这些节点。要运行这样的系统当然要付出成本，内容节点主机需用 ONE 去激励。

将 ONE 用作获取关注的货币

Menlo One 本质上是一门关注度经济。卖方或希望获得潜在顾客关注的某人既付费给内容节点，以便将资料页面传送给潜在客户，也付费给客户，以博取关注。典型使用场景有，Brave 浏览器与用户分享注意力变现后的收入 [8]，他们将浏览器内嵌广告网络中一定百分比的广告收入分配给用户。

将 ONE 用作良性激励机制

促进代币驱动型经济的代币驱动数据库

鉴于标准陈列式广告的价格相对较低，单个用户使用 Brave 浏览器或类似服务的创收可能不足以改变生活。将所有以往交易全部记录在不可篡改的账本上的另一个好处是可以轻松判定客户质量，并量化其关注度的价值。资深相关买家曝光的市场价值可能是当前常规陈列式广告的数百万倍。通常情况，许多用户会尽可能获得分享该广告收入的机会，甚至还会尝试新的在线社区。然而，如果没有机制防止爬虫等行恶者滥用系统，广告商可能对曝光的真实性丧失信心，从而导致网络价值降低。虽然传统上验证财务历史记录也算是审查客户资格的好方法，但它远不能抵御女巫攻击。

声誉证明

为了解决这些问题，我们想提出一种声誉证明算法（“PoR”）。PoR 是一种代币组织的声誉评分，由从生态系统的事件中接收信号的智能合约授予。该评分用于衡量用户想从曝光或其他可变现事件中获得的收益，例如采用同质代币（如 ONE），其相对于用户持有的不可替代声誉额。用户可以采取的声誉构建行为有贡献评论、帖子或评价，其价值由社区点赞数确定。点赞本身是值得为了激励参与而赢得声誉的行动。

PoR 与主流共识算法（如权益证明）形成鲜明对比。人们的声誉无法在其中购买或出售（在概念和技术上都是如此）。解决定量数学难题只会引发精英团体之间为争夺专业硬件和廉价电力使用权而展开军备竞赛，这是比特币的工作量证明算法存在的缺陷，其颇具讽刺意义。声誉证明被集中控制的风险较低，属于环境友好型算法，且使用起来相对较快。尽管目前 Menlo One 主要基于以太坊，但只要新网络可以同意迁移声誉余额，理论上可以将整个网络迁到其他区块链。

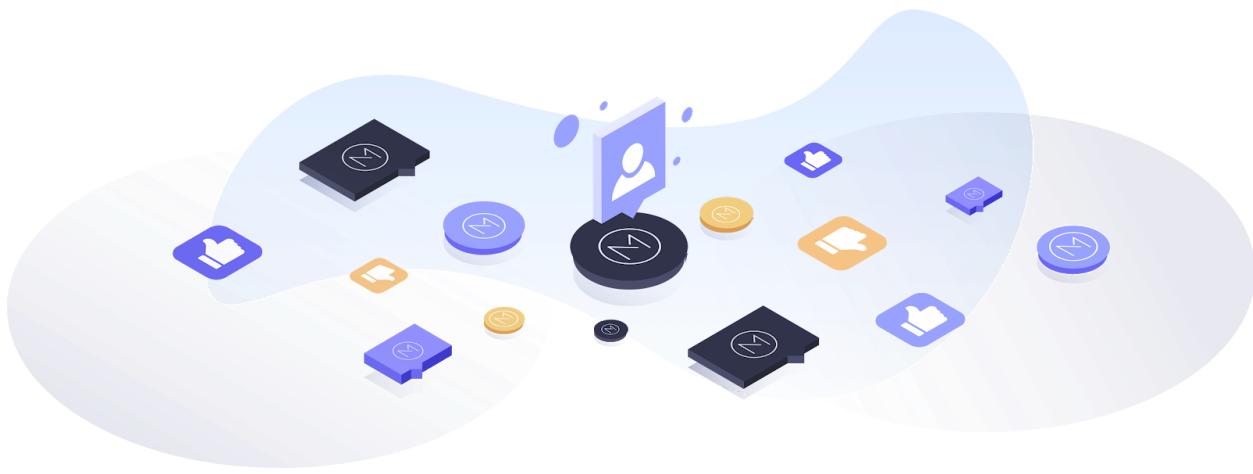
不少项目已在使用公链建立社会声誉。Userfeeds 利用类似的架构确定数据的相关性 [28]。最值得注意的是 Backfeed，其提出用声誉代币来建立用户对社区的贡献 [10]。若干押注身份的权威证明系统已被提出，与 PoR 有些相似之处，其中一个是出自以太坊联合创始人 Gavin Wood 之手 [29]。Menlo One 建立在这些系统和项目的基础上，以实施一种激励良性行为、抵制不良行为者、带来现代快速 Web 体验的系统。

先付出后获取的代币激励政策

Menlo One 和现实生活一样，通常先有付出才会有回报。鉴于声誉交易基于以太坊，新用户每次必须花钱购买 GAS，才能换取声誉赚取贡献。当然，激励机制是为了让用户建立足够的声誉以最终收回成本，最好可以赚取大量 ONE。内容节点在开始货币化之前具有更高的声誉阈值，因为内容节点应该投入到正确可靠信息的提供上。因此，参与者必须押注以太坊以加入此网络，并希望其能为生态系统创造价值。所有参与者均受到激励不对系统作弊。例如，若内容节点被发现服务于有效数据之外的任何其他内容，则将失去所拥有的声誉并立即丧失获利机会。

代币登记节点背景

代币登记节点 (TCR) 是新兴加密货币经济设计模式，参与者通过股权激励机制来管理列表。正如 TCR 发明人 Mike Goldin 所描述，“代币登记节点利用内在代币来分配与代币持有实体的代币相应权重成比例的管理权限。只要有参与方期望被纳入既定列表，就可以形成市场。市场中，对理性利己代币持有者的激励与管理优质列表的初衷一致。代币登记节点属于去中心化管理列表，对代币持有者具有内在经济激励，实现列表内容合理管理。”[9]。在 Menlo One 中，代币登记节点广泛应用于生态系统的许多方面，激励用户做出积极的增值贡献。



Menlo TownHall——通信层

Menlo TownHall 作为协议，用以促进去中心化、代币激励型通信系统。该系统内设一系列智能合约，并向为线上对话或讨论提供高价值信息的参与者给予 ONE 奖励。各参与者均为系统贡献 ONE。社区随后公布哪些消息具有最高价值或最相关。系统将对贡献价值最大的参与者分发 ONE 奖励。

在线聊天

大多数在线生态系统都有某种公共论坛功能。以财务手段激励具有深厚领域知识的专家来分享他们的见解，Menlo One 可用于创建生态系统，这些生态系统的用户生成内容质量高于其中心化的前辈。例如：该系统可用于奖励时薪上千美元的区块链开发人员，就某代币发行区块链公司的质量进行讨论，促成其贡献见解。

HashMail：私人付费消息服务

大多数在线生态系统都有私信功能。有了区块链技术，发送像 LinkedIn 的 InMail 或 Earn.com 等付费消息的难度会显著降低。将对称加密技术与智能合约相结合，用户得以为读取加密信息定价。

不可篡改性

许多在线市场均遭到所谓具有特权的管理人员审查不良评论或留言的指控。大家决定购买书籍等产品或者选择餐厅时，这种审查制度会带来不良后果。大家决定业务投资数千美元甚至数百万美元时，这种审查制度对投资者是不利的。若要确保对话不被修改，则必须建立不可篡改的论坛。

声誉

诸如点赞/点踩、打开消息或赢得奖励等用户行为可看做声誉迹象，TownHall 提供多种途径量化用户在网络中的声誉级别。

TownHall 内的代币经济

ONE 是生态系统内被用作为帖子、投票、以及奖励。以下是该生态系统的经济流动图。



TownHall 框架

我们打算将大部分产品作为自主独立产品发布，因为我们认为从面向对象的角度来看，使项目尽可能模块化是合理的。TownHall 的自主独立版本于 2018 年 4 月发布，可在以下位置获得：<https://github.com/MenloOne/townhall>。

TownHall 完全用 JavaScript (ECMAScript 6) 编写，旨在运行于最终用户的计算机。其通过 MetaMask、IPFS 等 web3 提供商与以太坊交互。为了更好了解 TownHall 如何与其他技术交互，我们从经典模型-视图-控制器架构的视角查看各项技术的角色。我们的 JavaScript 应用程序是视图层。TownHallJS 与以太坊上的智能合约均是紧密耦合的应用程序逻辑，从而相互协作实现功能，因此作为控制器。以太坊和 IPFS 均共享模型的角色。TownHall 为两个网络间的通信建立专有协议。

TownHallJS 应用程序

TownHall 旨在运行于最终用户的计算机。其大量采用 React JS 框架、webpack、及 IPFS、web3、Truffle 等依赖关系。TownHall 包含的界面刻意作为“空机”，而我们希望由最终用户开发人员依据自己的需求进行定制，并且我们希望此前演示的使用场景可使用该框架来创建。其需要将所有智能合约部署至以太坊，应用程序方能运行。

应用程序初始化后，其读取消息、投票信息及按配置文件规定地址存储于以太坊的其他数据。该步骤需要 web3 提供商和 IPFS 连接。一旦数据下载到本地，其会显示于 GUI 供用户查看。

身份验证与用户数据

最终用户实质上会用私钥为任何操作进行身份验证，其需要对系统作出发帖、投票、评论等写入操作。所有用户数据均与各自密钥关联。其中包括消息关联、投票计数、消息付款等。当然，还应将 Menlo One 代币付款至用户地址。

该密钥对身份验证设计模式在去中心化系统中司空见惯，尽管我们认为利大于弊，但并非无懈可击。其显著优势在于无需依赖中介机构就能实现身份验证，而缺点在于最终用户会丢失私钥或其私钥遭泄露。ERC20 标准适用于 Menlo 代币 (ONE) 的主要原因是为了便于代币转移。如果用户怀疑自己的密钥遭泄露，其可将自己的 ONE 转移至新建帐户。许多兼容 ERC20 标准的钱包还支持轻松创建易于备份、易于记忆的短语。至于如何负责任地处理，将密钥对用于身份验证再适合不过。尽管我们建议开发人员使用 Townhall 收集相关信息，便于最终用户了解如何负责任地存储和使用自己的密钥。

数据模型

话题、评论等基于文本的消息应遵循星际链接数据 (IPLD) 格式，然后由 IPFS 将其转换成简明二进制对象展现 (CBOR) 格式。IPLD 允许 IPFS 上的数据将所有内容可寻址数据结构视为一个大信息空间的子集，将数据作为 IPLD 实例与哈希关联的所有数据模型进行统一[104]。

消息 JSON 对象示例：

{

```
"version": <hash>,
"parent": <hash>,
"body": <string>,
"issuer": <pubkey>
}
```

TownHall 消息对象模型的结构 :

- 根
- 消息
- 话题
- 评论

核心功能

TownHall 有如下系统功能 :

1. 创建话题
2. 评论话题
3. 点赞话题
4. 点踩话题
5. 点赞评论
6. 点踩评论

TownHall 界面有如下功能 :

- 查看所有消息
- 提交新消息的输入框
- 点赞、点踩按钮
- “消息出售”按钮
- 消息发送“本帖已赚取 X ONE”文本

主要部件

Menlo 代币 (ONE)

说明 : Menlo 代币 (ONE) 是以太坊公链上的开源代币，其兼容 ERC20 标准。代币在系统内有多重用途，其中包括：1. 表示用户对话题有何等感受和 2. 用户如何在 TownHall 相互奖励。

ONE 是款举足轻重的软件，旨在与 TownHall 框架完美兼容，可以出售给开发人员，借以打造功能完善的产品。TownHall 及其他 Menlo One 产品与其他 ERC20 代币可交互操作，且购买 ONE 时，不应寄希望于 Menlo One 产品未来仅使用 ONE。

TownHallJS

说明：一款开源 JavaScript 应用程序。其与以下其他组件交互和协作。TownHallJS 负责与用户对接，为 IPFS 格式化数据，并与以太坊智能合约对接。

图形智能合约

说明：一款基于以太坊公用网络的开源智能合约，由 TownHallJS 将索引数据存储于该网络。Menlo Token 需要将条目存储于智能合约或与其交互。图形化合约包含消息节点间的链接。其创建和组织话题项下消息的图形化链接列表/树。其包含 IPFS 哈希对合约内索引的映射，以供消息对象使用。这图让用户整合出讨论板的概览。

投票和付款合约

说明：该合约将用于消息投票。如果用户在 24 小时内拥有点赞数排前 5 的消息，那么该合约用于将图形化合约收到的费用支付给用户。用户必须调用该方法才能申领奖励代币。如果用户未在 24 小时内申领代币，则代币会回滚入代币池。期限内的首位申领者将触发付款金额计算。

所有点赞和点踩必须用代币关联，因为代币用于表示投票者有何等感受。所有更新插入必须用 JSON 对象与论坛消息关联，而 JSON 对象包含签名和哈希。该付款结构将用于奖励 24 小时内排前 5 的消息：第 1 : 40%，第 2 : 25%，第 3 : 20%，第 4 : 10%，第 5 : 5%。

用户旅程 1：创建新消息

1. 用户希望创建新话题。
2. 针对用户评论，在本地分配一个 IPFS 内容可寻址哈希。
3. 该哈希随后与费用和父消息一同被发送至图形化合约。
4. 图形化智能合约请求固定费用的 Menlo 代币和以太币 (Gas)。
5. 用户在图形化合约中看到相应消息的元数据，那么用户会将消息发送至 Menlo 的 IPFS 实例。IPFS 确认消息后，Menlo Core 上的其他订阅者也会看到。
6. 其他用户能“点赞”或“点踩”消息，可能是话题，也可能是帖子，具体视用户认为消息向对话提供的价值有多大。
7. 每 24 小时，系统将确定排名前 5 的消息。发布热门消息的用户可调用投票和付款合约上的方法来兑换奖励。

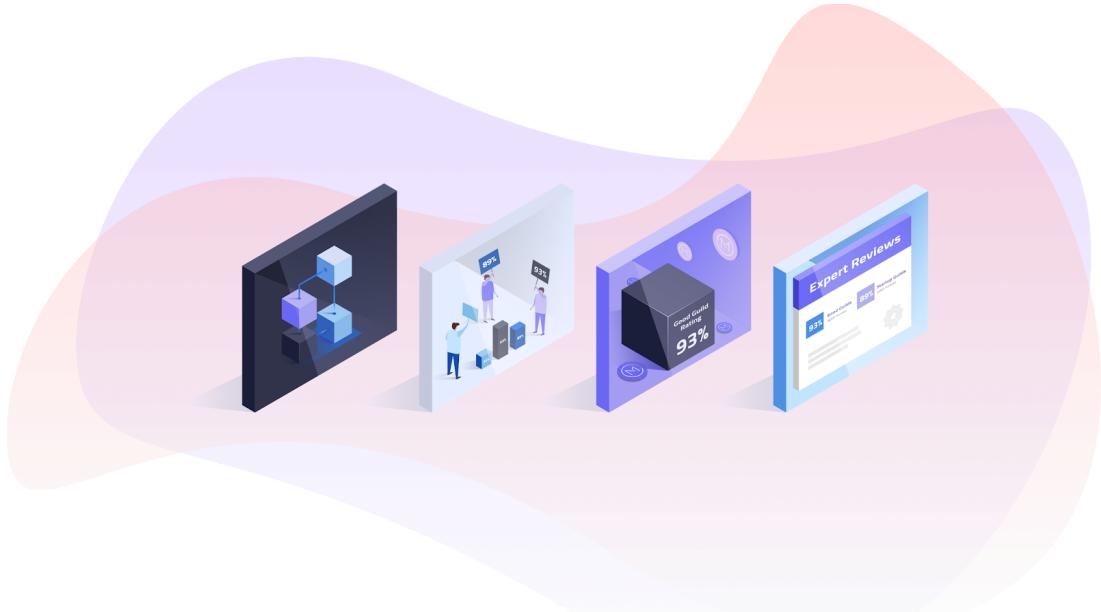
用户旅程 2：在留言板上给消息点赞

1. 用户看到自己喜欢的消息，并调用点赞方法。
2. 投票和付款合约内的方法被调用。需要少量 ONE 来调用方法。
3. ONE 存于投票和付款合约内，并且将进入奖励池。点踩所获的费用也将进入奖励池。

用户旅程 3：兑换发布话题所获的 ONE

1. 用户希望收集因创建热门消息而获得的 ONE。

2. 用户看到自己的消息在今天排名前 5，随后调用投票和付款合约内的方法。
3. 该方法检查调用的以太币地址是否与排前 5 的发帖人地址吻合，如果相同，则酌情付款。



Menlo Guild——治理层

设计考虑因素

设计该网络时，我们考察了针对传统在线评论（它们出了名的不准确）的许多替代方案。

我们原定的目标是：

1. 鼓励专业人士分享见解。
2. 减少在线点评中的腐败和贿赂。
3. 建立生态系统治理体系，以识别潜在的行恶者。

大量研究表明，财务激励是让用户发表评论的有效手段 [11]。我们还发现，对审查员分组可有效减少贿赂机会。斯坦福大学的研究表明，建立所谓“Guild”（协会）的去中心化社会结构（此概念可追溯到中世纪）可有效减少审查中的腐败现象 [12]。鉴于 Guild 与采纳智能合约的去中心化自治组织（DAO）[13] 有相似之处，以这种方式组织人员对区块链技术而言似乎顺理成章。

加入 Guild 后，会员参与讨论或提供反馈意见时会考虑同行的声誉及自己的声誉。

押注声誉的代币登记节点

我们提出的 Guild 是面向特定领域专家的系统，用于创建去中心化自治组织，便于成员建立代币登记节点 (TCR)，向市场用户提供专家意见。作为代币市场的实际示例：多位资深工程师联合成立名为“Developer Guild”的 Guild，用于审查 ICO。他们共同审查卖方的技术优势，并押上自己的声誉为社区提供优质评论。

卖方可以提交审查请求，并通过智能合约将一定数量的 ONE 托管给第三方（赏金）。任何数量的 Guild 都可以审查该卖方，但该卖方不能选择审查员。赏金中的 ONE 并非平均分配给 Guild，相反，报酬与 Guild 拥有的声誉数量挂钩。声誉越高，报酬就越高。Guild 必须提供有见解的优质评论，以获取足够的声誉，实现专业技能变现，提供劣质评论会导致 Guild 随后丧失声誉。

用于筛选搜索结果的质量信号使用

评分作为质量信号提供给用户以便筛选。每个 Guild 都可设置各自认为“合格”的阈值，每个 Guild 随后持有各自“合格”名单上卖方的 TCR。

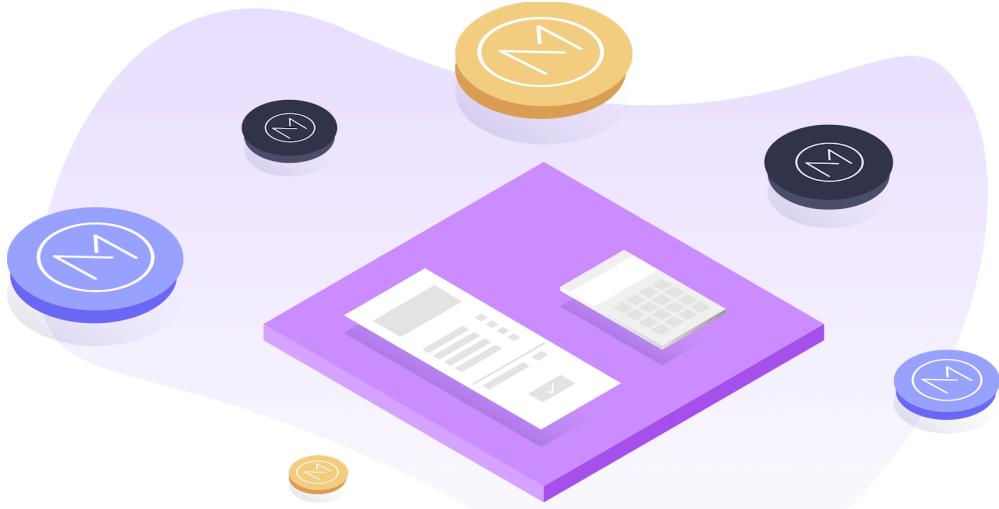
Guild 系统架构

Guild 是智能合约矩阵 Guild 会员资格存储在智能合约中。Guild 会员资格由投票决定，并通过智能合约完成。Guild 对问题的投票结果存储为 0-99 整数。所提问题的哈希将存储在投票智能合约中。Guild 也可以递交书面审查，必须获 Guild 三分之二成员同意，方可批准。Guild 可设置“合格分数”，被审查项目将列入推荐项目名单。

事实证明，这样的架构是利用智能合约作为工具来管理社交会员资格与治理的实用解决方案。例如，DAOstack [14] 拥有稳健的框架，并具有类似的架构和功能。

卖方可以通过押注 ONE 的某值来“质疑”审查结果。质疑让 Guild 有机会考虑遗漏信息或错误。如果 Guild 不接受质疑，其声誉将受损。对方案的投票结果决定是否接受质疑。如果质疑得到解决且错误得到纠正，则项目可收回其 ONE。如果质疑无需更改，则卖方 ONE 将发送至社区池。AdChain 已实施类似系统 [15]。

Guild 中一名或多名成员在审查中收受贿赂有被抓的风险。支付给 Guild 的 ONE 中有一小部分会进入“欺诈池”。社区成员可以押注 ONE，以质疑 Guild 受贿。如果社区投票证实此事，则欺诈池会进入社区池中，立即返还举报人押注的 ONE，同时 Guild 丧失其全部声誉。



Menlo Pocketbook —交易层

Menlo 智能钱包

集成智能钱包是交易层的核心，旨在改善用户的 dApp 使用体验。钱包集成了 API，允许使用 EarlyBird 协议进行自动化交易，并支持跨多网络交易。

预授权交易

无论交易大小，大多数现有 ERC20 钱包强制用户为每笔交易输入密码。我们认为密码机制妨碍了 dApp 和去中心化的普及。Menlo 钱包内置预授权交易 API，允许用户执行某些频繁操作（如评论、点赞等），无需授权每笔交易。为了确保交易安全，仅允许 Menlo One 生态系统内的地址使用此功能，同时用户可根据交易频率和成本限制这些互动。

自动买入

自动买入功能让用户能够制定计划，在未来某个时间执行交易。在 ICO 市场或节日票务拍卖使用场景中，该功能便于用户异步购买代币，而不必守在计算机前等待代币销售开始（这当然是种糟糕的用户体验）。钱包有一个 API，可接入智能合约，起到购买事件排队的作用。其将有助于用户制胜数分钟内销售一空的“哄抢”式销售，而是让买家从发售宣布的那一刻起渐进入场。该功能无需复制和粘贴智能合约地址，降低用户密钥处理不当或遭恶意软件攻击的风险。

1.从用户的角度来看，他们可以通过简单的“立即购买”按钮购买东西。其工作原理是利用 pub/sub 和我们称之为“EarlyBird 协议”的排序系统。卖方启用自动买入功能时，则将部署 EarlyBird 智能

合约，以便用户以愿意花费的以太币金额提交买入订单。这些预订按提交时间优先排序，并在此订单中执行。

2.买家设置 Menlo 智能钱包，了解 EarlyBird 合约中的事件，例如：销售区块编号、以太币接收地址，钱包将自动移至给定区块。每个用户将按顺序分配到区块编号。

3.如果项目尊重该系统，则将按协议规定的顺序处理订单。如果他们确实尊重此系统，则将因此获声誉奖励。

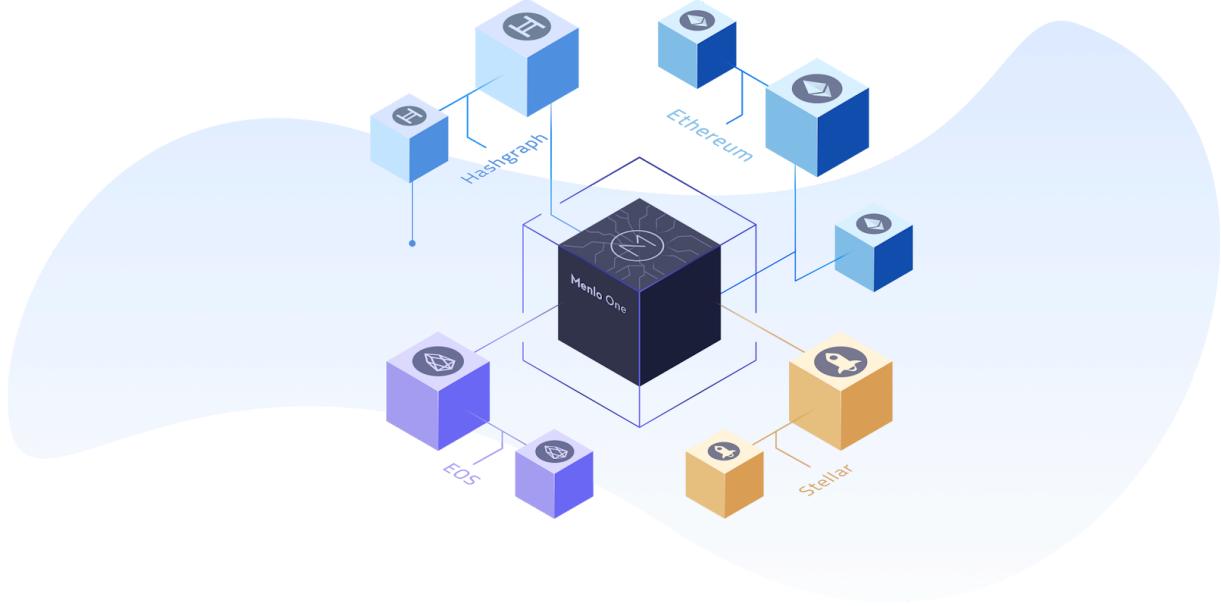
跨链互操作性

Menlo One 旨在向前兼容以太坊以外的智能合约区块链网络。撰写本报告时，以太坊仍是迄今为止最受欢迎的智能合约网络，但目前有 EOS、Stellar、Hashgraph 等若干项目可能对以太坊构成激烈竞争。管理多个钱包只会加剧分裂式用户体验。因此，Menlo 钱包允许将其他网络的轻量级副本下载至用户设备并在界面中列出代币销售，从而轻松采用这些系统。

从用户的角度来看，在以太坊网络购买代币或在 EOS 等其他网络的购买体验实际上是相同的。项目托管的网络将显示在界面上，但结帐体验基本相同。

KYC 身份管理

许多接受加密货币付款的卖方需要向买家索取文档，以符合 KYC/AML 规定。用户将政府颁发的身份证件和其他个人身份识别信息（PII）保存在他们的 Menlo One 钱包中。我们与某家领先的反洗钱背景调查供应商合作，授权其筛选投资者。数据将被加密保存，以便用户在需要将数据发送给某人。



Menlo Core——数据层

区块链协议以全新方式在去中心化、去信任环境中实现数据存储、分发和验证。而区块链理论上具有不可篡改性，有意利用其安全保障来设计现代 Web 应用难度不小。此外，基于云的 Web 应用为用户带来便利，如无需在本地下载所有数据即可进行查询。我们提出一系列系统和协议，其受益于区块链网络的安全保障、分布式数据存储的成本效率及传统 Web 服务器的速度和可靠性。市场建成后，内容节点可缓存从这两个网络提取的数据，并将数据传输至客户端，使用声誉证明算法刺激网络增长并降低出现不良参与者的风险。

- 对于数据存储，我们使用的是星际文件系统 (IPFS)，该协议旨在为存储和共享文件创造去中心化的永久方法 [21]，但数据缓存于用户操作的节点阵列，用于执行相应任务，例如不会给最终用户带来负担的查询。卖方为用户支付赏金以获取其关注，并付费使用内容节点数据。对内容节点和用户的奖励均基于采用声誉证明算法的智能合约，奖励大小与其声誉挂钩。它完全去中心化，没有单点故障，并以传统网络主机的速度提供区块链验证数据，因为内容节点很可能托管在 AWS 等高性能网络服务器上。

系统架构考虑因素

构建 Menlo Core 时考虑以下原则。

隐私保护

所有参与者应拥有假匿名使用该系统的选项，因为用户可能会发表不受欢迎的观点或披露对某公司或产品不利的信息。

消除中间环节

所有参与者必须能够在没有任何中间人（包括：许可系统的管理员）的情况下参与贡献。系统必须能够在没有单一中央服务供应商情况下仍然维持工作。

抗审查

系统应具有抗审查性，因为用户可能会发表不受欢迎的观点或披露对某公司或产品不利的信息。可过滤社区视其为不适宜的消息，但消息应永久保留。

优雅

系统必须拥有优雅的设计，促进有效沟通，同时便于用户部署，无需特殊硬件或招募数量庞大的参与者来确保其安全。

快速

系统必须具有足以实现向论坛异步发帖的速度，但不必具备实时聊天的速度。

负担得起

系统费用不应令大多数用户望而却步，且能购买互联网设备，就能用得起。

开源

为了保障安全实现其他考虑因素，系统必须完全开源。

关键术语

卖方：寻求他人关注，以便出售或推广产品、服务或品牌的个人或公司。卖方持有希望获得关注物品的资料。他们将 ONE 托管给第三方智能合约，以激励内容节点提供数据，并付费吸引用户查看其资料。

内容节点：托管的 Web 应用从 IPFS 和以太坊提取数据，包括：卖方资料及高性能计算机数据库中的缓存。

用户：收费查看卖方资料者。款项来自发布人列表合约。

声誉：适用于正面声誉的代币在本白皮书中，我们使用字母 PoR 来表示，但这些代币不能在系统之外转让，也不能在任何地方公开挂牌上市。根据使用场景，会有多种 PoR。

负面声誉：适用于负面声誉的代币

资料：卖方资料本质上就是卖方广告。

管理员 Guild: 类似于 DAO 的管理员小组，按劳动获得报酬。

Grantor：授予 PoR 和其他系统代币的智能合约。

验证器：验证交易的智能合约。

身份认证

所有参与方均使用以太坊密钥认证身份后进入系统。卖方使用密钥创建或更新资料。希望加入网络的新用户在注册时部署智能合约（全自动处理），其中含用户资料地址（存储于 IPFS）及声誉代币余额。这种密钥对身份认证设计模式在去中心化系统中正变得日益常见。Menlo 钱包还支持创建易于备份的助记短语。

关注度经济

Menlo One 关键在于赢得市场关注度。例如现实社会中，寄件人选择联邦快递寄包裹并支付快递费，并期望收件人打开包裹时也获得报酬。ICO 具体使用场景中，实体希望付费给内容节点，希望将资料传送给够买过代币的投资者。以电子书商店为例，作者愿意支付费用，邀请阅读量大的用户阅读其上架书籍。

使用以太坊验证存储于 IPFS 的数据

为了实现拜占庭容错的同时又能承受消息存储费用，协议同时运用以太坊网络和星际文件系统 (IPFS) [25]，在这两个去中心化网络间建立通信，弥补各自的局限性。星际文件系统是储存数据极具成本效益的系统、不过缺乏像太坊一样的网络安全保证。此外，IPFS 上的内容只能通过哈希索引。大多数用户希望按照名称或市场中其他密钥搜索内容。为实现优势互补，Menlo Core 将消息数据存储于 IPFS，将内容哈希存储于以太坊。尽管消息本身并未存储于以太网，但消息记录却存储于以太坊。

区块链存储动态内容的解决方案

区块链理论上具有不可篡改性，有意利用其安全保障来设计现代 Web 应用难度不小。基本 Web 应用必须具有动态内容，例如：易于更新的用户资料。我们将项目内容的引用保存为项目合约中的状态变量，以此解决这个问题。项目更新资料时，新内容将作为全新文件存储于 IPFS，而引用在智能合约中进行更新。假设无人访问旧数据，IPFS 将在 24 小时内将其自动移除。

通过缓存内容节点提升以太坊性能

我们提议构建自主以太坊和 IPFS 内容缓存市场，以解决上述难题。以太坊充当不可篡改的公用账本，没有任何中心化的协调者。内容节点和用户之间的交易记录由项目的 Granter 智能合约批准，内容预取和传送流程由内容节点完成。Granter 还提供关于网络中内容供求情况的可公开访问记录。

声誉证明激励

Menlo One 生态系统的核心是代币登记节点，为长期表现优异的参与者给予奖励。用户会被授予以不可转让的声誉代币衡量的代币化“声誉”。声誉代币的数量不设限。如下情况，Menlo One 生态系统给予用户 ONE 奖励：评论、加入 Guild 及内容节点提供数据。ONE 可转让，可作为货币。我们将来可能使用多种类型的声誉来衡量特定指标。

为了防范行恶者，声誉证明算法确保系统奖励用户的 ONE 数量与其地址持有的声誉挂钩。例如：具有极少声誉的恶意爬虫不会因查看资料而获得用 ONE 支付的报酬。然而，TownHall、Guild 和其他声誉授予系统的活跃用户在查看卖方资料时会获得用 ONE 支付的报酬。

激励后的内容节点网络

Menlo One 上的所有数据均存储于 IPFS，而该数据的哈希存储于以太坊。为了向用户以媲美传统 Web 应用的速度和体验提供数据，我们将存储于 IPFS 传统数据库、由内容节点上 Web 应用提供的数据缓存起来。系统中有许多内容节点竞相提供数据。内容节点向用户提供资料来赚取 ONE，并收取一定比例的卖方款项作为服务费。内容节点可为每笔成功交易构建声誉。系统有多个内容节点，不会出现单点故障。

收到内容节点提供的资料时，用户也可从 IPFS 中提取相同的数据以核实真实性。高声誉用户可向管理员 Guild 报告恶意内容节点。为确保内容节点使用 Menlo One 社区提供的 Web 服务器代码，内容节点的文件系统必须公开。用户可提取内容节点代码，然后与存储库中的副本核实哈希，从而赚取声誉。

用于资料查看的 Granter 智能合约

一旦在 Menlo One 上创建资料，资料数据便会存储于 IPFS，卖方的 Menlo 钱包在以太坊上部署了内置 Granter 智能合约，其中包括 IPFS 托管资料的内容可寻址哈希。项目还将 ONE 发送至 Granter，作为资料查看的赏金。为了便于在系统中查看资料，对 Granter 持有的 ONE 数量并没有最低要求。但是，内容节点对于系统提供的自动买入等“高级”功能可相应收取费用，因为运行这些功能会花费内容节点的计算时间。其实，该机制为数据可用性提供了动态开放市场。

Granter 愿意支付的最高限价由 Granter 中的卖方设定。由于受制于市场价格波动，卖方可随时修改 Granter，以改变其价格。资料的流量自然将决定内容节点的市场价格。卖方资料越受欢迎，服务费就越高。

检索证明

卖方用 ONE 支付报酬，激励内容节点传送资料。因此需要运用检索证明机制，其要求内容节点和用户均必须对资料哈希进行数字签名，并将其提交给 Granter。为了激励用户支付交易所需的 gas 汽油，我们给予用户预定比例的 ONE 报酬。

使用激励型 Validator 缓解攻击向量

1. 恶意内容节点已篡改 IPFS 提供的数据。

通过引入中间内容节点，我们创造更改数据的机会。存在多个检索证明类系统旨在确保外包供应商传送的数据不会被第三方审核员更改 [22][28]。在我们系统中，用户使用 Granter 检查数据的有效性，因为用户和内容节点必须均已提交已签名的交易用于支付报酬，但是用户可能在一两分钟时间内认为该被篡改的数据是真实的。

我们采用自主 Validator 网络降低这种屡见不鲜的风险。用户从内容节点中接收资料时，会在本地为资料生成哈希。用户和内容节点均向 Granter 提交数字签名的有效负载。如果用户提交的内容哈希与卖方存储于 Granter 的哈希不匹配，则向接受订阅的 Validator 发布事件。这些 Validator 是针对问题内容节点运行请求的节点。

如果内容节点返回被篡改的数据，则 Validator 向内容节点发放负面声誉代币。其直接内嵌于 Granter 协议中，不会向拥有负面声誉的内容节点支付 ONE。系统中建立足够声誉可能需要工作数周或数月时间。任何声誉变现之前，运行内容节点需预付费用。丧失变现能力的威胁激励内容节点杜绝不良行为。

2. 篡改搜索结果的内容节点

为了实现快速搜索，我们并不要求各用户托管数据库本地副本。内容节点一项关键功能是从副本中快速查询数据的能力。Menlo 开发社区决定搜索结果背后的算法和参数，以确保系统中每个人的公平性。风险在于内容节点可能会篡改查询结果，也许是为向其他人推广或审查某次特定的代币销售。

作为运行内容节点的部分规则，文件系统应始终可读。Menlo 钱包具有从文件系统中提取内容并在本地进行哈希运算的功能，用户随后将其与来自公共存储库中的代码库哈希对比。如果用户发现内容节点代码与存储库有任何不同，则用户向 Validator 发布事件，Validator 也会进行检查。如果 Validator 也确认内容节点正在运行未经批准的代码，则向其发放负面声誉。只有 Validator 具有授予负面声誉的权力，并由 Validator Granter 合约授予声誉，以激励执行这些任务。必须有三分之二的 Validator 达成共识，方能将负面声誉分配给潜在行恶者。

系统架构组成部分

Menlo 客户端应用

这款原生桌面应用可在用户计算机上运行。其包含捆绑在 Electron 内的 JavaScript 界面应用。其承担若干责任。

- 提取前端代码存储库的最新副本。
- 服务于前端应用。
- 从内容节点列表合约中发现内容节点。
- 将客户端直接连接到内容节点。
- 纳入以太坊轻量节点供所有交易使用：购买代币时将以太币转移至智能合约，以及与 Menlo 交互，包括：创建用户资料、点赞卖方资料、使用 TownHall 进行评论。
- 从 IPFS 中提取数据并验证该数据与内容节点提供的数据相同。
- 为所有交互验证用户身份（通过以太坊密钥）。
- 从内容节点签署数字签名作为响应，索取查看发布人资料应得的赏金。
- 未来将纳入 EOS、Stellar、Hashgraph 等其他区块链。
- 保存用户的 KYC 身份证明（已加密）。

Menlo 节点应用

Menlo 节点应用属于 Node.js 应用，含服务于 JSON 的 RESTful API。内容节点从 IPFS 抓取应用数据并存储于本地数据库，以便用户快速访问。其提供多项用户功能，例如：按密钥查询，而非按 IPFS 内容可寻址哈希。内容节点必须保持文件系统上所有内容的开放性，且任何人均可读（不包括含密钥和其他敏感数据的文件），便于用户审核文件系统。GitHub 上大多数最新代码的哈希必须与内容节点上的哈希匹配。内容节点必须承担服务器费用和列表费，方能参与网络、赚取 ONE 和构建 PoR。

- “列表合约”适用于用户待发现的内容节点。
- 内容节点必须每 24 小时用 ONE 支付一次费用，方能保持列表状态。用于支付 IPFS 定位成本。
- 列表合约告知用户其 IP 地址、声誉和其他元数据。
- 内容节点必须托管存储库中最新的 Web 应用代码。

智能合约矩阵

这些智能合约运行此系统并充当 Granter 提供 PoR 奖励。

- 列表：列出可用内容节点
- 资料 Granter：确认资料传送并授予 PoR

代币经济学

系统内的 ONE 流

1. 卖方将 ONE 放入以太坊上的列表合约。合约包含在 Menlo 应用中。

2. 用户向节点请求资料时，将自己的公钥放入请求中。内容节点返回数字签名作为响应。双方随后将各自的密钥和数据提交至卖方列表合约。
3. 如果成功，则双方获得 ONE 付款。用户因别人关注而获得报酬。内容节点因数据可用而获得报酬。
4. 卖方列表合约也是 PoR Granter，并因成功交易而给予各行为人声誉代币。

用户赚取 PoR 的方式

用户可以多种方式赚取声誉，包括：成为 TownHall 中的顶尖评论者、在 TownHall 中投票、加入 Guild，以及通过 Menlo 钱包进行链上购买。各系统均由具有 Granter 特权的智能合约运行，以提供声誉。内容节点通过长期提供可靠数据来赚取声誉。

Menlo Core 使用场景

有人愿意付费确保别人看到某物时，该系统就是理想之选。例如：Alice 愿意付钱给 Bob，以确保将某物交付给 Charlie。例如现实社会中，寄件人选择联邦快递寄包裹并支付快递费，并期望收件人打开包裹时也获得报酬。

在线广告等现有若干商业模式适用。Brave 浏览器是本项目的灵感来源，其理念为：广告观看者也会获得部分广告收入，以换取其关注。然而，Brave 目前使用信任型中介服务，从而有能力负担小额支付需求。完全去中心化的代价通常是成本和速度。Menlo 将以太坊用于二进制文件传输，但用户兑换广告酬金的 gas 费用会超过广告本身的酬金。

其他项目已提出激励缓存区块链数据服务器的类似系统 [23]。然而，尚无法证实某些关键组件切实可行。例如：Menlo Core 声誉系统提供的适当激励结构，以及大多数区块链钱包糟糕的用户体验。像 Menlo One 这类代币化市场的出现意义重大，因为其充分考虑了涉及交易所的声誉和工具。

代币、ICO 或证券市场为这类系统提供了完美使用场景。一直以来，为了向相对少数的客户群体推广代币销售，许多公司耗费数十万乃至数百万美元。他们愿意花费大量资金，确保客户（他们可能支付数百万美元）看到产品。此外，最终用户将愿意支付构建声誉的前期 GAS 费用，以获后期较好激励。

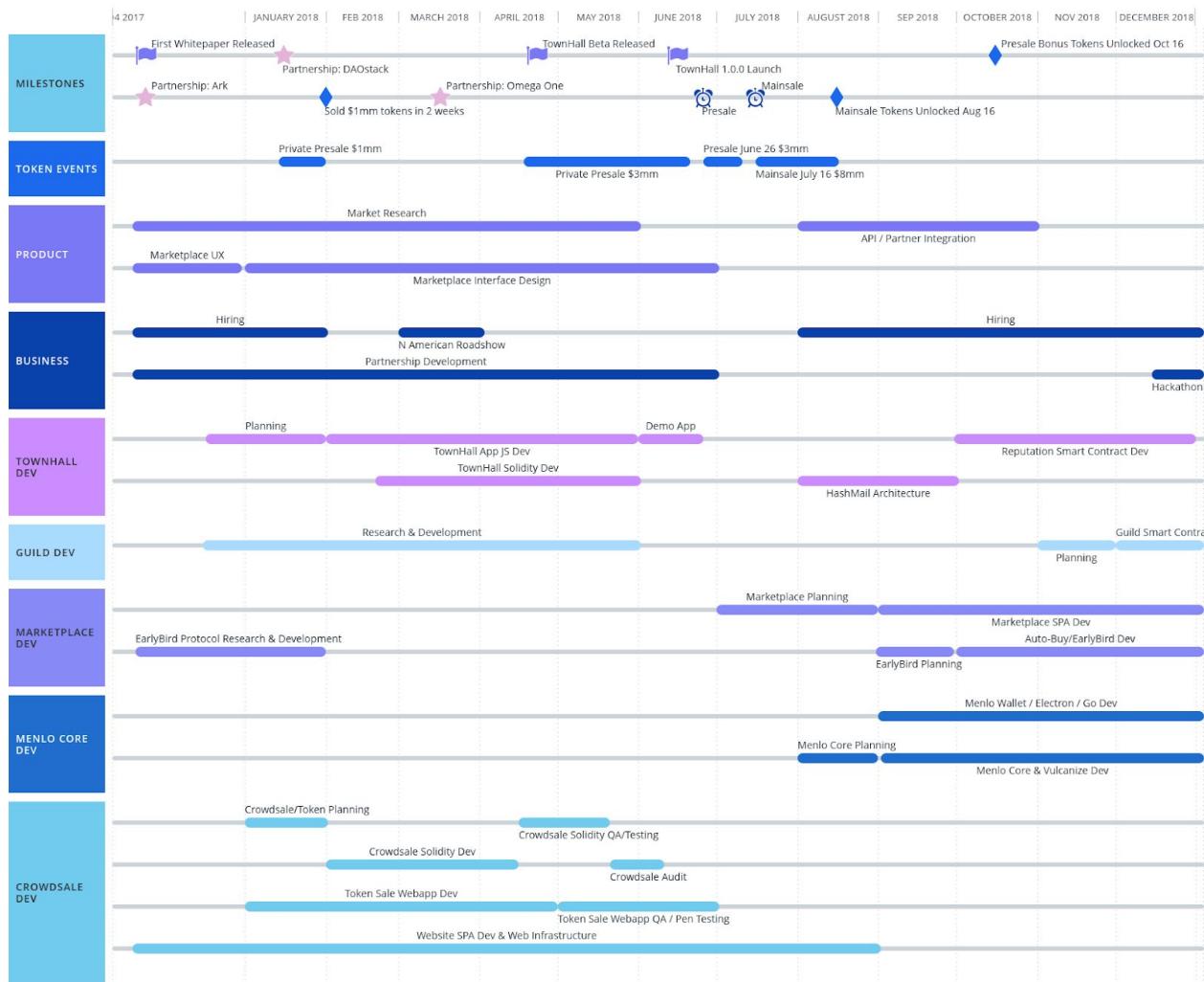
平台开发路线图

早期历史（2016-2017 年）

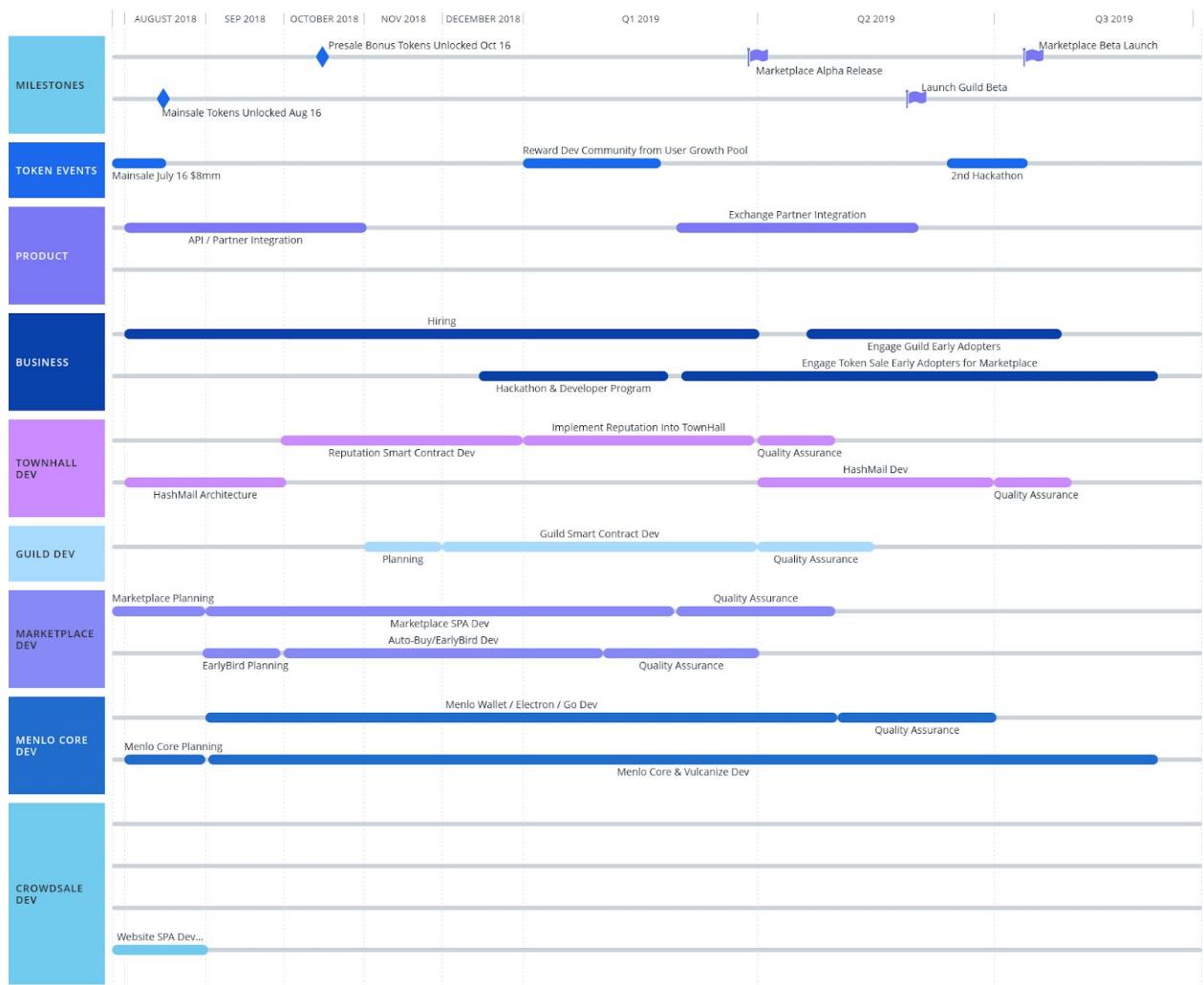
- 2016 年夏季：推出 TownHall 的前身 Ether-Signal。于 2016 年夏天专为以太坊基金会成员而开发，旨在帮助社区投票决定 DAO 入侵之后是否分叉。
<https://github.com/MenloOne/ethersignal>
- 2016 年：Vulcanize 的早期开发，这是由 Menlo One 团队成员发起的项目，也是 Menlo Core 关键所在。<https://github.com/vulcanize/VulcanizeDB>
- 2017 年：市场研究快速增长的区块链市场。对类似于 Menlo One 的产品需求日益清晰。

路线图（2017-2018 年）

注意：我们是精益创业方法论的坚定信徒。功能交付日期为预估，可能随用户反馈或其他因素而变化。有关路线图的更完整版本，请参阅此链接 <https://menloone.docsend.com/view/ky6hw8t>。



路线图（2018-2019 年）



团队

- **Matthew Nolan (首席执行官/工程) ([LinkedIn](#))**

连续创业家及全栈开发人员。曾任职首次代币发行顾问 Ark Advisors 的合伙人。Speek (2015 年被 Jive 收购) 联合创始人。摩根大通银行前高级工程师。IBM 前高级工程师。在 High 5 Games 建立过一些最大在线赌场。Verona (被《Fast Company》杂志评选为 2016 年度“最具创新力公司”) 创始人。全球公认的社会企业家，被 BBC、NBC、FOX 和 Vice 等媒体广泛报道过。2016 年威比奖获奖者。TED 演讲者及表演家。

- **David Dawson (首席技术官/工程) ([LinkedIn](#))**

David 在微软产品指导工程组织，对象包括产品和软件工程师，是具备 15 年经验的资深人士。他提供的产品为 Windows、Xbox 和 Office 提供动力，从可扩展的企业服务到消费者移动产品皆有覆盖。他还共同创办了 Mast Mobile 并担任首席技术官，专注于专门向 Hearsay Systems 出售的商业移动通信服务。

- **Tiaan Wolmarans (首席运营官) ([LinkedIn](#))**

Tiaan 是一位专注于运营和产品开发的企业家。他直接为多个 ICO 撰写了白皮书并为其开发了产品，这些 ICO 通过私人和公开发售众筹了 1100 万美元，还包括一些仍处于即将开始状态的 ICO。他还致力于 Hempcoin 的产品开发和重新推出以及 Solaris 的重新推出、开发和区块链迁移。

- **Marcie Grambeau (营销和传播) ([LinkedIn](#))**

Marcie 是一位多方位的营销和传播专家。她经验丰富，从计划、执行到生产和咨询，涉及健康、娱乐和科技领域的各种产品和服务。她是充满激情的品牌和初创企业倡导者，过去与 ARK Advisors 合作，通过 ICO 流程为包括 OmegaOne 和 Sn.ip 在内的公司提供支持。

- **Rick Gross (工程) ([LinkedIn](#))**

Rick Gross 从 9 岁起开始编程，12 岁开始自由职业生涯，13 岁实习，高中毕业后直接入行。过去 6 年里，他供职于 VML、High 5 Games、IPsoft 等知名公司，负责领导 Lexus、Korean Air、Mastercard.com 等品牌的开发工作。他在人工智能和劳动力自动化领域成功帮助推出广受认可的平台。

- **Dave Hoover (区块链架构师) ([LinkedIn](#))**

Dave Hoover 于 2015 年跳进区块链的“兔子洞”，很快就找到了通往以太坊的道路并一直专注于此。他曾在 ConsenSys、IDEO 和 Augur 工作，并作为审计员、工程师和指导为许多以太坊项目做出了贡献。Dave 是 Obtiva、Mad Mimi 和 Dev Bootcamp 的合伙人/所有者，上述公司全部被成功收购。Dave 合著有“Apprenticeship Patterns”《学徒模式》一书。

- **Felix Watkins (工程) ([Github](#))**

Felix 是业界公认的区块链开发专家，编写和审计智能合约，帮助数十个代币成功发售。Circles Seller 前创始人。

- **Brandon Carlson** (工程) ([LinkedIn](#))

Brandon Carlson 在构建部署定制 Web 应用程序方面拥有十多年经验。他先后任职于财富 100 强公司、美国政府、医疗保健和就业背景考察行业，从事安全基础设施开发工作。

- **Courtney Zalewski** (设计) ([LinkedIn](#))

Courtney 为许多科技公司设计过作品，包括 One Second Everyday (苹果 App Store 中排名第一)、Glimpse 和 Pager。

- **Ian Welch** (业务开发) ([LinkedIn](#))

Ian 领导了多家硅谷软件和生物技术公司的业务发展。他之前在 Raymond James 担任执业财务顾问，领导客户获取事务。

- **Nathan Windsor** (业务开发) ([LinkedIn](#))

Nathan 是 RChain 等项目的早期贡献者，也是 Macroscape 创始人。

顾问

- **Richard Titus (业务) ([LinkedIn](#))**

Richard D., "Titus", Ark Advisors 合伙人, 是具有全球经验的资深高管, 拥有逾 20 年数字化转型经验。他共同创立 11 家公司、包括 Prompt.ly 以及数码代理巨头 Razorfish (LA) & Schematic。他还领导过 Samsung Electronics、DMGT (Associated Northcliffe Digital 旗下 Daily Mail) 以及 BBC 业务部门, 其业绩受到 CES、全球移动通信系统联盟、Techcrunch 和华尔街日报的广泛认可。他于 2017 年为众多成功的 ICO 提供咨询, 其中包括 : Adex、Hive Seller、Pillar、Po.et、Guardium、Omega One、Reveal.it、Sun Exchange 以及 Sn.ip, 共募集超过两亿美元资金。

- **David Langer (资金) ([LinkedIn](#))**

创业合伙人 @ Pioneer Fund、出质人 @ Founders Pledge、导师 @ Seedcamp, 创始人/CEO @ Zesty Inc., David 是一位连续创业者, 活跃天使投资人和创业顾问, 合作公司 20 余家。

- **Mike Norman (业务/众筹) ([LinkedIn](#))**

Mike Norman 是大众投资平台 Wefunder.com 的联合创始人。拥有超过 6000 名出资人和 1600 万美元的启动资金。迈克帮助制定了 JOBS 法案的众筹部分, 并在白宫旁观奥巴马签署该法案。他拥有麻省理工学院斯隆管理学院的 MBA 学位。

- **Jill Richmond (营销) ([LinkedIn](#))**

Jill Richmond 是 SparkPR 旗下 Sparkchain 团队领袖。SparkPR 是业内顶尖企业, 其客户有 Blockchain Capital、Civic 及 Simple Token。她拥有超过 15 年经验, 并专注于初创企业, 包括联合创立两家公司, 并为世界银行集团创新实践部私营和公共领域提供全球创新支持。Jill 在众多会议和专题讨论会担任过策划人和发言人, 目前是福布斯、BTC 和 Distributed Media 常任撰稿人。她在《华盛顿邮报》、《VentureBeat》、《纽约时报》、英国广播公司、《Modern Luxury》、《BTC Media》、《福布斯》、《Spectator》等媒体上发表过对技术和创新的独特见解。

- **Marissa Kim (法律) ([LinkedIn](#))**

Marissa 是 Ark Advisors 合伙人、证券和资本市场律师, 她专注于帮助区块链和加密生态系统的创新者启动项目、筹集资金, 以及引导和影响监管环境。此前, 她服务于大型金融机构和财富 500 强企业, 从事上市公司和私人公司交易实践的各方面工作, 专注于公司金融、股票公开上市和内部认购、企业并购, 并为纽约市的 Skadden、Arps、Slate、Meagher & Flom, LLP 组建了对冲基金和私募股权基金。

- **Markus Ament (战略) ([LinkedIn](#))**

Markus Ament 是金融科技行业的连续创业者, 人称 Maex, 他成功带领众多初创公司发展成全球领先企业, 深受全世界成千上万人的喜爱。 Maex 现任 Taulia 首席战略官兼联合创始人

，将 Taulia 从 2009 年的公司构想发展成业内领先的金融供应链公司，与其他公司一起创建具有更高效率和盈利能力的供应链。Taulia 令人艳羡的客户名单包含众多财富 500 强企业，有 300 多名员工，已快速成为金融供应链中公认的领导者。

- **Elissa Shevinsky (产品) ([LinkedIn](#))**

Elissa 是连续创业者，担任过 Brave 浏览器产品负责人以及 Glimpse 首席技术官。她撰写过有关网络安全政策方面的文章，并在 HOPE 等安全活动中发表过演讲。Elissa 是《Lean Out》的作者。

- **Mike Hostetler (工程) ([LinkedIn](#))**

Mike 是连续创业者，现任 Raise 区块链总监、Modern Web 首席执行官、SuperBetter 首席技术官及 jQuery 卖方负责人。

- **Jake Baval (社区) ([LinkedIn](#))**

Jake Baval 又名 Korean Jew Trading，资深加密货币企业家，从零开始建立草根社区，以帮助人们驾驭此领域为使命。他在社区发展和建设方面经验相当丰富，也经历过 ICO 投资困境，其深刻洞见对于 Menlo One 平台及其用户友好型功能的开发具有巨大价值。

最重要的增长因素：开发者社区支持

软件开发的历史反复表明，产品成功的关键在于开源的固有网络效应。Linux 崛起之初，许多固守传统的商界人士冷嘲热讽，一群去中心化的业余程序员竟痴心妄想他们的产品可与云软件行业当时的龙头老大微软竞争。这个开源项目不仅启动了，而且据估计，现在超过 75% 的互联网运行于 Linux 之上，取代了中心化巨头微软。社区广泛采纳显然为该免费软件带来商业优势，以抗衡当时世界上最赚钱的生意。

区块链运动加速这些网络效应。比特币是终极开源项目，其技术创始人至今仍是谜。尽管有许多拥有出色团队和强大领导力的项目许诺开发更快、更便宜的比特币，但就市值而言比特币仍是一枝独秀。第二大加密货币是以太坊。以太坊创立之时存在多个智能合约项目。在我看来，以太坊成功的首要原因在于他们的社区建设努力远胜于其他。他们在许多城市举办见面会，次数超过其他项目。我们如今撰写本白皮书是因为部分 Menlo One 成员参加了 2014 年以太坊见面会。

Menlo One 的成功并非仅取决于创始团队，我们能做的毕竟很少。我们只能擦出燎原之火花。和其他成功的开源项目一样，成长取决于开发人员是否接纳。构建本项目时，我们力争在各方面完全去中心化。我们的目标是，即使出于某种原因，Menlo One 团队不再从事该项目的工作，它也会继续运转下去。虽然本文的意图并不在于呼吁开发人员的支持，但我们鼓励任何对 Menlo One 感兴趣的人士以各种方式参与该项目。软件开发本质上是团队运动。

项目治理结构

所有项目均遵循“自由”开源贡献模式。在自由贡献模式下，通常认为贡献最多的人士最具影响力，但这是基于当前工作而非历史贡献。重大项目决策是基于共识寻求过程（讨论重大不满），而不是纯粹的投票，并尽量听取更多的社区观点。使用自由贡献模型的其他项目范例还有 Node.js 和 Rust [24]。

Menlo 代币发售

为了促进生态系统发展，我们将举办代币销售活动。部分数字可能随以太币/美元汇率波动而变化，但以下数字为最优预估值，即 1 以太币 = 600 美元。ONE 与以太币挂钩。我们的众筹合约公布于我们的 Github ([链接](#))。

指标	说明	建议值
主要销售日期	主要众筹日期	有待公布
硬上限	资本筹集总额及大概的市场发行价值	1,500 万美元/25,000 枚以太币或达到硬上限
挂钩比率	以太币/ONE 关系	1:12,000
价格	1 枚 ONE 代币的价值	0.000083 枚以太币
代币发售总数	供应的代币数量	3.54 亿枚
代币总供应量	代币铸造总数	10 亿枚
T1 价格奖励	内部预售 > 100 万美元	50% 奖励
T1 价格奖励	内部预售 < 100 万美元	40% 奖励
T2 价格奖励	公开预售	30% 奖励
T3 价格奖励	众筹	浮动折扣
锁定 (预售)	仅锁定奖励代币。其余在代币销售结束时发放。	公开发售开始 90 天后；发售结束日 60 天后
锁定 (团队)	针对所有代币的锁定时间	2 个月锁定，然后 2 年授予。
锁定 (顾问)	针对所有代币的锁定时间	2 个月锁定，然后 1 年授予。
未售代币	未达到硬上限的剩余代币	耗尽

代币发售阶段

层级	说明	总筹资额（百万美元）*	总筹资额（以太币）	售出的代币数量（百万枚）

T1	内部预售 (TPA)	4	6,667	116
T2	公开预售 (白名单/KYC)	3	5,000	78
T3	众筹 (白名单/KYC)	8	13,333	160
		15 百万	25,000	3.54 亿枚

* 用美元计的总指标为预估值，且假定 1 以太币 = 600 美元

代币发售奖励结构（主要公开版）

为了激励买家尽早购买，我们将提供代币奖励。代币折扣以代码形式写入众筹合约（[链接](#)）。

- 第一小时（即“动力小时”）七折优惠
- 第一周八折优惠
- 第二周八五折优惠
- 第三周九折优惠
- 第四周九五折优惠

代币发放

代币分布以代码形式写入众筹合约（[链接](#)）。

- 众筹销售的代币：35.4%
- 代币用于公司未来发展：24.6%
- 代币用于 Menlo One 团队：20%
- 代币用于 Menlo One 合作伙伴：10%
- 代币用于 Menlo One 顾问：10%

参考文献

- [1] <https://blog.chainalysis.com/the-rise-of-cybercrime-on-ethereum/>
- [2] <https://medium.com/@altcoinio/slack-api-for-icos-de61df6448c3>
- [3] <https://medium.com/crypt-bytes-tech/ico-hack-coindash-ed-dd336a4f1052>
- [4] Estimate based in part on number of downloads of Metamask, a popular ERC-20 compatible wallet.
<https://chrome.google.com/webstore/detail/metamask/nkbihfbeogaeohlefnkodbefgpgknn?hl=en>
- [5] <https://www.forbes.com/sites/jonathanchester/2017/08/16/your-guide-on-how-to-run-an-ico-for-better-or-worse/#4a9645973c58>
- [6] <https://themerkle.com/top-5-ethereum-wallets-compatible-with-cryptocurrency-ico-tokens/>
- [7] <https://github.com/ethereum/eips/issues/20>
- [8] <https://basicattentiontoken.org/BasicAttentionTokenWhitePaper-4.pdf>
- [9] <https://medium.com/@ilovebagels/token-curated-registries-1-0-61a232f8dac7>
- [10] https://github.com/Backfeed/documents/blob/master/whitepaper_objective_protocol.pdf
- [11] <https://hbr.org/2018/03/online-reviews-are-biased-heres-how-to-fix-them>
- [12] <http://hci.stanford.edu/publications/2017/crowdguilds/guilds.pdf>
- [13] <https://blog.ethereum.org/2014/05/06/daos-dacs-das-and-more-an-incomplete-terminology-guide/>
- [14] <https://daostack.io/wp/DAOstack-White-Paper-en.pdf>
- [15] <https://adtken.com/uploads/white-paper.pdf>
- [16] https://github.com/Thetta/GitBook_ICO-Approaches
- [17] <https://ethresear.ch/t/explanation-of-daicos/465>
- [18] <http://people.cs.uchicago.edu/~teutsch/papers/ico.pdf>
- [19]
https://medium.com/@Vlad_Zamfir/a-safe-token-sale-mechanism-8d73c430ddd1#.xq1pyiyia
- [20]
<https://media.consensys.net/exploring-continuous-token-models-towards-a-million-networks-of-value-fff153175776>
- [21]
<https://ipfs.io/ipfs/QmR7GSQM93Cx5eAg6a6yRzNde1FQv7uL6X1o4k7zrJa3LX/ipfs.draft3.pdf>
- [22] <https://eprint.iacr.org/2009/281.pdf>
- [23] <https://arxiv.org/pdf/1801.07604.pdf>
- [24] <https://opensource.guide/leadership-and-governance/>
- [25] <https://github.com/ipfs/ipfs/blob/master/papers/ipfs-cap2pfs/ipfs-p2p-file-system.pdf>
- [26] <https://www.ethereum.org/>
- [27] <https://github.com/vulcanize/VulcanizeDB>
- [28] [https://userfeeds.io/Userfeeds_Protocol_Whitepaper_\[Draft\].pdf](https://userfeeds.io/Userfeeds_Protocol_Whitepaper_[Draft].pdf)
- [29] <https://github.com/ethereum/guide/blob/master/poa.md>

致谢

感谢 Joshua Landau、Wendy Brawer、Tiaan Wolmarans、Marcie Grambeau 和 Mike Hostetler 对本白皮书提出宝贵意见并予以修订。感谢 DAOstack 带来有关 DAO 架构的许多灵感。感谢 Rick Dudley 早在 2014 年就向我介绍了以太坊。非常感谢 Menlo One 团队。感谢 Menlo One 社区与我们共同发展代币经济，并创建了加密货币领域气氛最热烈的 Telegram 小组。

保留所有权利。

版权所有 2018, Menlo One Inc.

免责声明：

本文仅用于提供一般信息之目的，并可能随着平台的日渐发展而修改。Menlo One 或 ONE 无意构成任何司法管辖区的受监管产品。本解释性说明并不构成购买 ONE 或 Menlo One 代币的建议，任何缔约或采购决定也不应依赖于本说明。有关更多详情，请参阅 [https://menlo.one/。](https://menlo.one/)

[了解更多信息](#)

satoshi@menlo.one | www.menlo.one