

OpenAIChain

白皮书

Open AI Chain 链致力于打造共享人工智能平台

目录

目录

术语表.....	5
1. 理念背景	6
1.1 背景概述.....	6
1.2 AI with Blockchain 理解	6
1.2.1 价值传导	6
1.2.2 数据模型信息对称.....	7
1.3 OpenAIChain 设计愿景.....	7
1.3.1 分布式人工智能生态环境.....	7
1.3.2 分布式生态中“水源” --OpenAI Token (OAT)	8
2. 架构及技术.....	9
2.1 OpenAIChain 总体架构.....	9
2.1.1 系统架构	9
2.1.2 底层区块链	11
2.1.3 共识机制	11
2.2 CDPOS 共识算法与选举机制.....	12
2.2.1 共识算法设计.....	12
2.2.2 区块产生及验证.....	12
2.2.3 共识过程	13
2.2.4 分叉选择	14
2.2.5 风险分析	14
2.3 智能合约虚拟机与授权管理.....	15
2.3.1 虚拟机	15
2.3.2 合约 AI 接口.....	16
2.3.3 合约授权管理.....	17
2.3.4 合约资金担保.....	17

2.3.5 合约模型验证.....	17
2.4 分布式算力与存储机制.....	17
2.5 模型存储和数据隐私保护.....	18
2.5.1 模型存储.....	18
2.5.2 数据隐私保护.....	19
2.6 基础服务及开发工具.....	20
3. 关键技术.....	20
3.1 OpenAI Rank 指数.....	20
3.1.1 指数总设计.....	20
3.1.2 排名算法.....	21
3.1.3 抗操纵能力.....	22
3.2 激励机制.....	22
3.2.1 奖励及分配算法.....	22
3.2.2 分中心节点激励机制.....	22
3.2.3 全网节点激励机制.....	22
3.2.4 验证节点激励机制.....	23
3.3 区块链搜索引擎.....	23
3.3.1 搜索基础架构.....	23
3.3.2 关键词搜索.....	23
3.3.3 模型算法搜索.....	24
3.3.4 趋势榜单.....	24
3.4 GPU, CPU 分布式训练.....	24
3.5 分中心节点溯源链.....	26
3.6 智能合约升级设计.....	27
3.6.1 合约调用 AI 即服务.....	27
3.6.2 合约抗风险能力.....	27
4. OpenAIChain 生态驱动.....	29
4.1 面向全人类--数据激励驱动平台.....	29

OpenAIChain 链致力打造共享人工智能平台

4.2 面向学习者--知识分享平台	33
4.3 面向高校及科研工作者--资源协作平台.....	35
4.4 面向多领域--打造区块链切实落地项目	35
4.4.1 配合教育领域打造区块链机器学习应用落地项目	35
4.4.2 学术工程溯源打造标准.....	36
4.4.3 智能人才招聘.....	37
4.4.4 算法竞赛服务.....	37
4.5 面向企业用户--打造贡献算力存储平台.....	37
4.6 面向开发者--资源整合平台	38
5. 代币销售众售规则	39
5.1 OpenAI Coin（OAC）代币发行.....	39
5.2 代币分配方案.....	39
5.3 代币销售规则说明.....	39
6. 应用和未来工作.....	40
6.1 应用案例.....	40
6.1.1 数据交互服务.....	40
6.1.2 信息社交服务.....	40
6.1.3 跨学科交叉服务.....	40
6.1.4 人工智能应用.....	41
6.1.5 竞技比赛	41
6.2 未来工作.....	41
7. OpenAIChain 发展规划	41
7.1 开发路线图.....	41
7.2 未来迭代规划.....	42
7.2.1 底层架构迭代.....	42
7.2.2 商业应用迭代.....	42
8. OpenAIChain 治理架构	42
8.1 基金会设立.....	42

OpenAIChain 链致力打造共享人工智能平台

8.2 基金会治理原则..... 43

8.3 基金会组织架构..... 43

8.4 基金会人力资源管理..... 44

8.5 基金会风险评估及决策机制..... 44

9. OpenAIChain 核心团队成员..... 44

10. OpenAIChain 顾问..... 45

10.1 技术顾问..... 45

10.2 学术顾问..... 46

10.3 商业顾问..... 46

10.4 合作机构..... 47

11. 投资机构..... 47

12. 免责声明与风险提示..... 47

术语表

- PoW Proof Of Work 工作量证明
- PoS Proof-Of-Stake 权益证明
- BFT Byzantine Fault Tolerant 拜占庭容错算法
- DPOS Delegated Proof-Of-Stake 授权股权证明
- CDPOS Contribute Proof-Of-Stake 贡献股权证明
- PoC Proof-of-Capacity 容量证明
- NLP Natural Language Processing 自然语言处理
- AI DApps Decentralized Artificial Intelligence Applications 去中心化人工智能应用
- EVM Ethereum Virtual Machine 以太坊虚拟机
- PS Parameter Server 参数服务器
- HE Homomorphic Encryption 同态加密
- FHE Full Homomorphic Encryption 完全同态加密
- ECC Elliptic curve cryptography 椭圆曲线密码学
- SGD Stochastic Gradient Descent 随机梯度下降法
- ASGD Asynchronous Stochastic Gradient Descent 异步随机梯度下降算法
- SL Supervised Learning 监督式学习
- UL Unsupervised Learning 无监督学习
- SSL Semi-Supervised Learning 半监督学习
- RL Reinforce Learning 强化学习
- SVM Support Vector Machine 支持向量机
- CNN Convolutional Neural Network 卷积神经网络
- RNN Recurrent Neural Network 递归神经网络
- DNN Deep Neural Networks 深度神经网络
- PR Pattern Recognition 模式识别
- AR Augmented Reality 增强现实

1. 理念背景

1.1 背景概述

2008 年 10 月 31 日，比特币[1]开启全新伟大的 P2P 时代，其创世设计驱使参与者维持其运转，全网参与者均为数字价值交换监督者，使得交易双方可以在无需建立信任关系的前提下即可完成交易。2015 年 6 月 30 日，以太坊[2]作为区块链 2.0 时代，为区块链交互提供图灵完备编程语言，将每次与区块链的交互作为交易信息写入区块链中，解决比特币网络脚本语言过于简单和扩展性不足的问题。2018 年 6 月，作为区块链 3.0 的 EOS^[3]正在等待一个有缘人开启来迎接区块链百万 Tps 时代。于此同时，近年来大热的大数据快速发展，以概率统计为基础的机器学习、深度学习在工业界以及学术界大受追捧，并在视觉、语音、自然语言、生物识别等领域获得重要应用。但区块链与机器学习之间的相互结合项目确实寥寥无几，OpenAIChain 作为下一代区块链平台，致力于将区块链技术与人机智能领域结合，旨在建立全球数据激励、论文溯源以及知识分享平台。

1.2 AI with Blockchain 理解

1.2.1 价值传导

信息技术和互联网发展到今天，各种系统应用使得协同变的越来越便捷和高效，但是由于数据协同问题的存在，这种高效的协同绝大多数存在于一个企业或者一个组织内部。当不同的企业之间进行协同的时候，使用的方法和工具又回到了 20 年前的技术，绝大多数的数据协同仍旧在使用传统搜集手段，系统的对接其实并不是想象中那么简单。由于涉及到数据安全、商业机密、合作信任等方面的问题，这种对接不仅仅是一个技术问题。在效率和成本两方面都有着市场亟需的改进空间。

区块链技术可以帮助我们建立一种新型的、可信任的 (Trust-free)、激励性的，让各个参与方的协作在保证数据、知识共享的更加便捷和通畅，进而通过更加及时准确的信息流的支持，让在这样的生态环境中的价值传导可以伴随商业活动的开展并发执行，提支持更多的人工智能生态发展。

1.2.2 数据模型信息对称

我们认为区块链技术则可以继续打破这样的一种数据、知识不对称，让数据使用权最终归属于 AI 领域开发者、算法思路更加开源于 AI 开发者、学术领域更加公开透明。对于这种新型的点对点、有偿激励以及不可更改网络而言，将对业界生态产生光明影响。如果将未来变革生产力之首称为人工智能，那么大数据则为生产要素，其中的桥梁则为区块链。同样，人工智能不仅仅是各个公司，更多的是学习者，科研工作者，如何让全民参与，是 OAC 一直致力于解决问题。

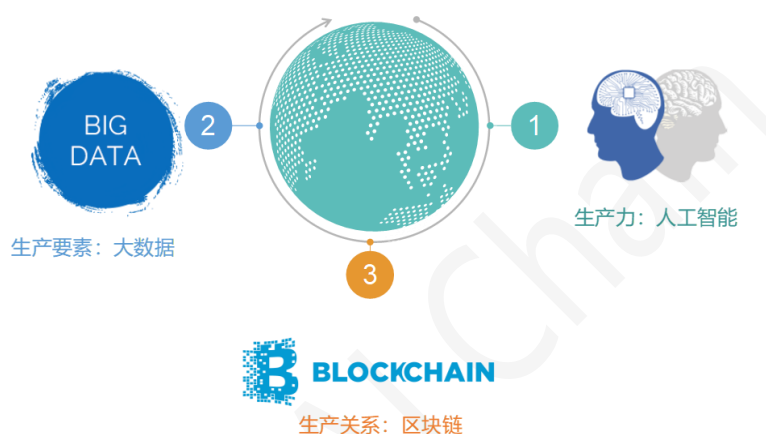


图 1.OpenAIChain 借助区块链搭建人工智能与大数据桥梁

1.3 OpenAIChain 设计愿景

1.3.1 分布式人工智能生态环境

(1) 愿景一：构建全民数据采集平台

OpenAIChain 针对当前人工智能发展的最大难题在于数据量，如何让开发者拥有更多数据量来提升自身模型精确度的行业痛点难题，借助区块链激励政策搭建生产力（人工智能）与生产要素（大数据）之间桥梁。OpenAIChain 将打造成全球最大数据收集平台，使全网用户通过区块链激励政策贡献全民数据，打造用户数据节点平衡。

(2) 愿景二：构建 AI 知识分享、问答平台

OpenAIChain 通过紧抓人工智能人才培养痛点，无足够开源算法分享、算法交流特点，打造运行在区块链上的开源社区软件，通过区块链激励政策有偿奖励知识分享者，形成自身 AI 开发社区，AI 算法仓库。

OpenAIChain 链致力打造共享人工智能平台

(3) 愿景三：高校论文溯源平台

OpenAIChain 旨在构造论文溯源，通过分中心节点运行机器学习论文项目，通过 OpenAIChain 智能合约系统判断训练精确度、存储模型及其训练参数，提升期刊论文公信度，杜绝高校论文造假现象。

(4) 愿景四：共享算力、存储平台

OpenAIChain 通过节点竞选方案提供一个基于共识的、分布式的节点计算、存储 AI 基础平台，使 AI 开发者、高校用户及科研工作者不受设备影像训练自身模型。

(5) 愿景五：模型、算法交易平台

OpenAIChain 打造提供算法、模型交易、程序交易平台，通过知识付费思想让算法不再闲置于计算机硬盘，而是发挥出其在特定领域作用，AI 开发者通过平台更可获得可观收入。交易平台通过官方智能合约系统认证，以确保交易可靠性。

(6) 愿景六：跨领域多方合作平台

OpenAIChain 致力于将多学科人才互补，打造各高校、科研院所联系关系，将人工智能领域与多个学科融合，打造高校自然科学论文与人工智能结合，提升中国高校科研交流。

(7) 愿景七：人工智能教育项目

OpenAIChain 致力于对个人教育溯源，与各地区中小学合作，记录成长轨迹，对学生成绩记录，科学分析学生个人成绩痛点。与各地区教育局合作，打造区块链落地项目。

1.3.2 分布式生态中“水源”--OpenAI Token (OAT)

若将整个分布式商业生态比作渔业生态，那么区块链就是水源，水源中的各种数据就是各种渔业资源，这样的生态一定需要水源，这个水源就是吸引各种珍贵鱼类巡游的关键--OpenAI Token (OAT)，承载着整个区块链网络及各种商业活动运输功能。OAT 同样我们会称为 OAC，主要作用是尽可能流通，让各个参与方使用，所以我们会出售一定量的代币到社区、企业、用户。

1) 企业、用户可以作为投资者在一开始付出 ETH 获取 OAT，ETH 交给 OpenAI 基金会平台技术开发、校企合作、数据采集以及提供区块链服务支持等；

2) OpenAI 基金会向各个数据、模型、算法代码片购买方收取 OAT，保障平台稳定运行以及知识分享。所收取的 OAT 收入的 40%作为分中心节点奖励，支付给节点提供商，40%作为数据、代码片分享者奖励，剩余的用于 OpenAI 基金会后续日常运行、商业推广和技术

开发；

3) 为企业、用户提供 DaaS（数据即服务）、AI 即服务和学校用户、个人开发者提供算力即服务，根据各自商业规则及附加价值贡献收取 OAT 来完善社区生态；

2. 架构及技术

2.1 OpenAIChain 总体架构

2.1.1 系统架构

OpenAIChain 作为 AI 底层公链，本质上是构建 AI 的基础设施、智能经济生态。对于区块链底层公链设计来说，我们考虑以下原则：

1. 扩展原则：底层各模块之间低耦合，系统适应新模块添加，每个模块本身更新不应该需要其他模块接口的变化。

2. 均衡原则：由于用户访问流量波动性，若大量用户访问到一个节点的时候，必然会带来节点的服务崩溃，所以节点的容器本身应该可以自动化部署，当用户请求出现压力的时候可以快速的实现横向扩展。

3. 隐私原则：OpenAIChain 生态的各方参与者，人工智能开发者、高校用户、人工智能厂商、科研工作者可以得到隐私保护，参与者可以根据自己的需求来选择性开放权限。

OpenAIChain 链致力打造共享人工智能平台

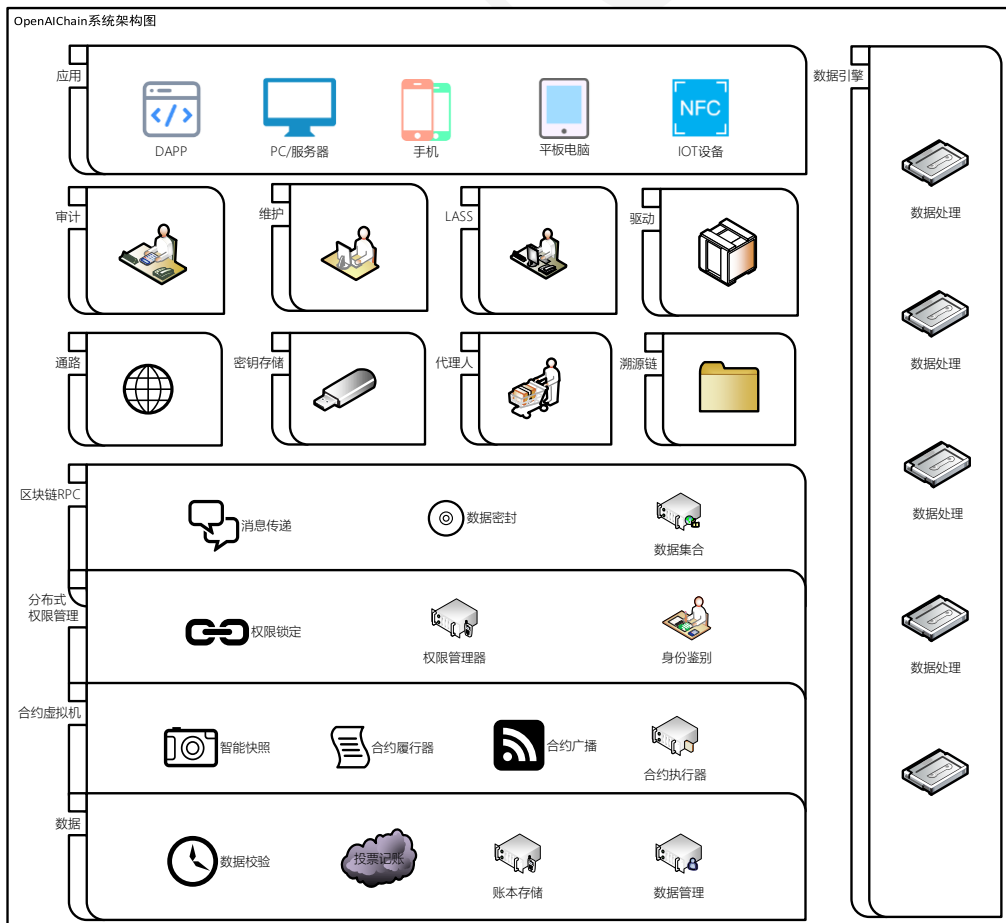
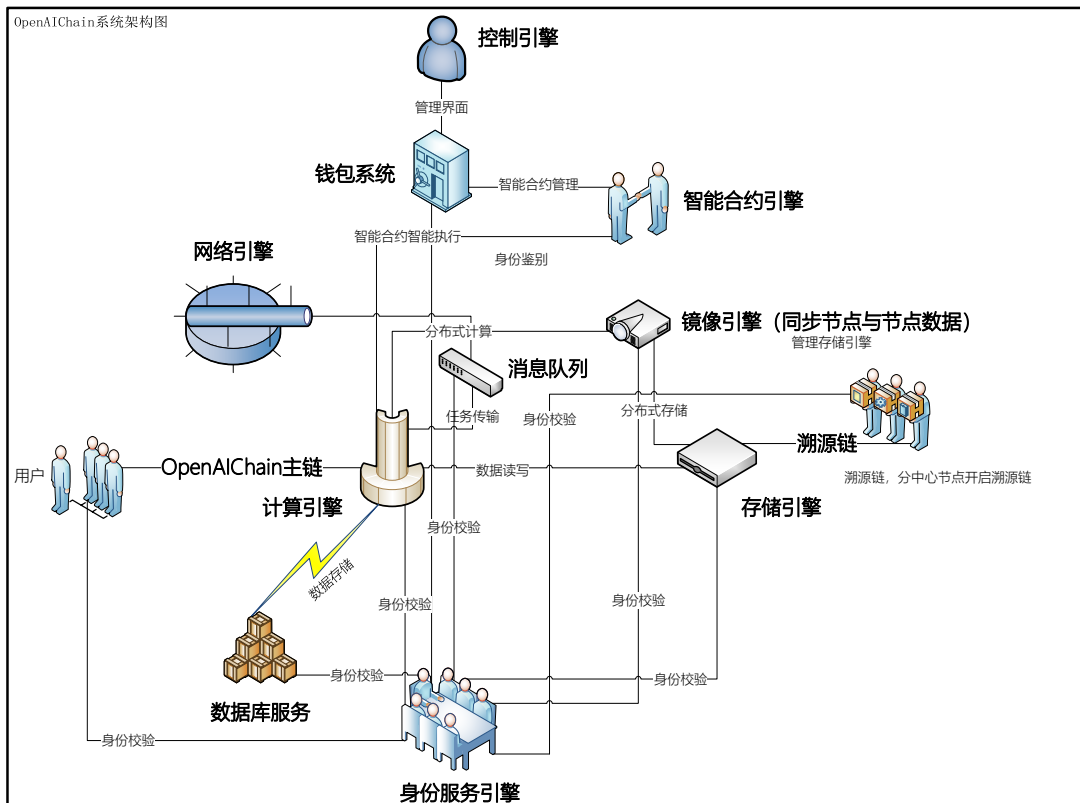


图 2.OpenAIChain 系统架构图

OpenAIChain 链致力打造共享人工智能平台

应用区块链技术开发系统，可省去中间环节，提供激励机制，提高生产积极性。在软件架构方面，IBM 把传统的 MVC (mode, view, control) 设计模式 (design pattern) 变为 MVBC (model, view, blockchain, control) [16]。目前，在区块链应用中单链结构往往会导致账目、合约、交易等同时存储于同一条区块链中，单链设计不符合实际 AI 领域需求，没有保护隐私，这种架构造成系统上存在大量异种数据，违背软件工程设计原则。随着业务、节点增加，通信量将会非常庞大，延迟增大，性能降低。OpenAIChain 在改进 EOS 源码情况下对分中心节点开启溯源链服务，有效降低查询成本，保护数据隐私，详细请见 3.5。

1) 控制引擎 (ContEngine)：用户通过控制引擎与 OpenAIChain 之间进行交互，在 OpenAIChain 中，分为用户钱包界面及开发者界面。

2) 计算引擎 (CalcEngine)：单用户或群组用户请求提供算力服务，负责模型运算的创建、挂起、暂停、调整、重启以及销毁等操作。OpenAIChain 将提供一系列验证接口，当用户提交分布式 AI 训练任务至计算节点，模型训练后，提交至智能合约引擎进行模型验证。一旦模型准确率达到预期标准，断定为训练完毕，否则，由钱包系统提交至用户。

3) 智能合约引擎：提供基础智能合约服务以及 AI 智能合约服务。

4) 镜像引擎 (DEngine)：同步节点之间全网服务数据，通过节点请求判断是否与同步数据相关，将请求转给镜像管理寄存器服务，镜像管理寄存器会解析请求数据内容，并和数据库交互存取和更新镜像数据。

5) 存储引擎 (SEngine)：存储各种对称加密模型数据。

6) 身份服务引擎 (IEngine)：为 OpenAIChain 其他服务提供身份认证和信息认证功能，管理命令、项目、用户等工作。

7) 网络引擎 (NEngine)：提供全网网络李连杰服务，为服务用户提供接口，可以定义网络、子网、虚拟 IP 地址，并使得节点之间负载均衡。

8) 数据库服务引擎 (DEngine)：为用户在 OpenAIChain 环境提供可靠备份引擎和非关系数据库服务。

2.1.2 底层区块链

OpenAIChain 底层区块链，具备如下特点：

1、底层整合 EOS 源码，以利用其高吞吐量特点。通过整合 tensorflow、CNTK 提供分布式 AI 训练接口，从底层重新构造公链，支持高性能以及分布式 AI 模型训练。

OpenAIChain 链致力打造共享人工智能平台

2、主链+溯源链组成。各地区分中心节点须开启溯源链，其主要功能用于学术论文溯源，验证其是否造假，溯源链模型、算法以及数据存储利用加盐后 IPFS 所得哈希。

3、OpenAIChain 的通讯传输采用自编码解释的二级制传输协议或者二级制加密传输协议，减少网络带宽，并且同一链路的不同消息包的编解码协议可以自由切换，提升传输的安全性。

2.1.3 共识机制

比特币虽然模型简陋，但其通过运用数据加密、时间戳以及分布式共识^[7]有效解决了拜占庭将军共识问题^[8]，实现节点无需信任的分布式系统中去中心化点对点交易，但其出块速度慢，Tps 低等特点让比特币无法成为数字货币系统基石。分布式环境下，数据为保证一致性需要使用一致性协议。大多数公有链主要采用工作量证明（Proof of Work）^[1]和股权证明（Proof of Stake）^[6]机制，许可链中主要使用 PBFT 及 CBFT。一般而言，区块链系统越告诉越好，但是共识代价昂贵，许多算力及节点都花费在共识机制上。如 PBFT 需要 3 轮投票，每轮投票及交易都需要签名和解签，因而 80% 的计算力都花在共识处理上。OpenAIChain 独创 CDPOS（Contribute Delegated Proof-of-Stake），将用户权益、用户网络贡献结合起来进行评估，采用分层流水处理，存储、共识、验证流水化分层处理，提升整个网络的系统伸缩性。CDPOS 模块中加入传统的 Kademlia 网路搜索算法，结合用户地理位置，针对用户不同地理位置添加不同权重，从而让各地区节点联系更为紧密，提升整体网络传输效率，使得交易和区块在最短时间内广播至全网每个节点，最终达到百万级 Tps。

2.2 CDPOS 共识算法与选举机制

2.2.1 共识算法设计

共识方面，OpenAIChain 起初论文溯源思想源于比特币 PoW（Proof of Work），采用哈希运算来确定记账人，整个挖矿过程中 PoW 无故消耗大量算力资源，且区块产生速度受限。而 Ethereum 已在将 PoW 转换为 Casper^[26]来作为升级目标，但 PoS 是以股权（资本）来证明记账率，大集团资本一方面能维持生态币价稳定，另一方面，与“公平性”背道而驰。

OpenAIChain 设计共识算法时结合考虑 CAP（Consistency, Availability, Partition Tolerance theorem）定律和 FLP 原理，提出 CDPOS 机制，融入了 SVN (Social Value Unit) 因子，创造

OpenAIChain 链致力打造共享人工智能平台

性地实现了 CDPOS(Contribution Delegated Proof-of-Stake)算法，有效避免了目前投票机制中的贿选、联盟投票，小号海投等弊端。CDPOS 类似于董事会投票，由官方在各省高校、知名企业选取一定数量节点，进行验证和记账。为激励更多企业高校参与竞选，系统会生成代币作为奖励，若投票选出节点在规定时间内 T 内无法履行职责，则会被除名，网络会选取出新节点来取代。其中，最后记账节点依据节点所分担的流量高低来决定，如下式所示， W_{tx} 是该中心地理范围内交易次数， $W_{transfer}$ 是分中心节点处里多少计算任务分发、存储任务分发， W_{ps} 是一定时间内高校论文提交训练次数，提交次数， α 、 β 、 λ 分别为权重参数。

$$f(t_0) = \alpha W_{tx} + \beta W_{transfer} + \lambda W_{ps}$$

2.2.2 区块产生及验证

先观察 OpenAIChain 中的区块结构，然后讨论如区块验证问题。

区块结构 OpenAI 链区块数据结构包含，但不限于以下信息：

- Block：区块
 - Id：区块 id
 - Schedule_version：时间戳版本
 - Height：高度
 - ParentHash：父区块哈希值
 - Checksum_type 交易的默克尔树根
 - StateRoot：状态根哈希值
 - TxRoot：交易默克尔根哈希值
 - ActionRoot：执行动作默克尔根哈希值
 - TransNum：交易数
 - Singnature_type：见证人签名
 - Accoun_name：见证人排序版本号
 - Producer：区块生产者
- Transactions：交易数据（包含多个交易）
 - From：交易发起人地址
 - To：交易接收人（普通用户或智能合约）地址，对于智能合约地址，值为 0

- Value: 转账金额
- Data: 交易的 payload, 若交易为创建智能合约, 则为智能合约字节码; 若交易为智能合约调用, 包含调用函数名称和入参值
- Signature: 交易签名
- Nonce: 交易唯一性标识
- Votes: Prepare 和 Commit 票数统计 (包含多个), 用于 CDPOS 共识算法中
 - From: 投票人
 - VoteHash: 投票区块哈希
 - HeightVote: 投票区块所处高度
 - VoteType: 投票类型, Prepare 或 Commit
 - Signature: 投票签名
- Region_summary: 区域
 - Cycles: 串行, 多个 Shards 组成一个 Cycles (周期)
 - Shards: 并行, 多个 Transaction 组成一个 Shards (片区)
 - Transactions: 交易数据

类似其他数字加密货币系统, 用户和区块链互动都是通过特定的交易进行的。用户创建一笔交易, 使用自己私钥签名后, 发送到地理位置最近节点中, 通过 P2P 网络广播到全网节点。在固定出块时间间隔内, 由 CDPOS 算法指定的记账节点打包这段时间内所有交易, 生成标准格式区块, 并同步到全网所有节点中。

2.2.3 共识过程

新的区块被提出后, 当前稳定节点验证者集合中所有人将会参与一轮 BFT (Byzantine Fault Tolerant) 方式的投票, 来确定此区块的合法性。接下来进入两阶段投票过程。

· **第一阶段**, 所有验证者需要对新区块投 Prepare 票, 如果当前阶段超过 2/3 的验证者对新区块投 Prepare 票, 则区块进入投票的第二阶段。

· **第二阶段**, 所有验证者需要对新区块投 Commit 票, 若当前验证者投了 Commit 超过 2/3 后, 那么该区块到达 finality 阶段。

为加速这个过程, 如果区块的 Prepare 和 Commit 票时间戳和区块 b 的时间戳时间超过指定时间 T, 那么这些投票将被视为过期投票, 直接忽略。

2.2.4 分叉选择

CDOPS 算法以每个高度区块的得分来选择权威链，总是选择得分最高的区块加入权威链，在高度 h 的区块 b 的得分如下：

$$Score(b, h) = \sum_{(b', h') \in children(b)} Score(b', h') + \sum contributed\ deposit\ in\ b$$

Contributed deposit in b 即为该区块最近收到的所有数据、算法、模型提交频率，后选择 Score 值最大的那条链，从而避免分叉。

2.2.5 风险分析

OpenAIChain 网络设计旨在将重点放在分布式点对点事物操作优先性上，将上一代区块链设计的速度和安全性作为重点考虑事项。设计时会将 CDPOS 网络与 EOS 漏洞作为重点考虑。

远程攻击 (Long-Range Attack)

类似于比特币中的 51% 攻击，攻击的远不止几个区块，在 CDPOS 中，攻击者可以伪造一个写在区块链上的合法交易，同时将这个相同交易写到最接近网络初始的另一条链中。OpenAIChain 希望通过确保所有区块都有标记时间并且通过 Score 函数来防止远程攻击。一旦在区块链上发现不正当行为，该协议将攻击者从网络剔除。

2.3 智能合约虚拟机与授权管理

2.3.1 虚拟机

我们将引入 LLVM^[23] 做为 OVM 的核心组件，并使用 LLVM Byte Code 做为 OVM 字节码。OVM 字节码通过 LLVM JIT 完成动态编译和优化，运行在 OVM 沙盒环境中。在这种架构设计下，OpenAIChain 的核心代码、智能合约能直接享受到 LLVM 带来的性能和安全性不断提升。

LLVM 早期是 Low Level Virtual Machine 的缩写，是一系列高度模块化的编译器和工具链技术的集合，包括 Google、Apple 在内的公司都使用它做为代码编译框架。LLVM 提供了一

OpenAIChain 链致力打造共享人工智能平台

套中立的中间表示 (LLVM IR) 和相应的编译基础设施, 并围绕这些设施提供了一套全新的编译策略, 包括对 LLVM IR 的化、LLVM IR 到不同硬件平台的代码生成、LLVM IR 到 LLVM Byte Code 的代码生成以及 LLVM Byte Code 在不同硬件平台上通过 LLVM JIT 直接执行。依托 LLVM 构建 OVM, 提供区块链底层 API 库。OpenAIChain 将改造 LLVM 提供主流语言支持虚拟机, 同样兼容 EVM, 帮助合约开发者快速搭建 DAPP。

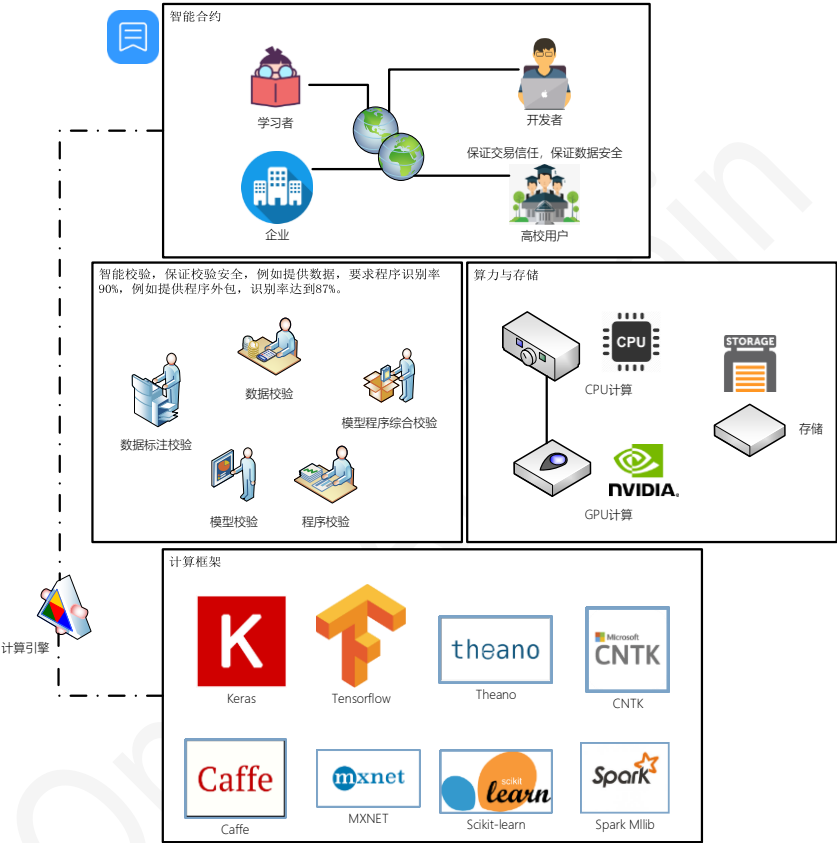


图 3.OpenAIChain 智能合约框架图

2.3.2 合约 AI 接口

当前企业、超算中心拥有较强的独立算力, 愿意将这些算力开发给 AI 创新企业, 一方面可以利用闲置算力提供收益, 另一方面可以在服务过程中提升自己计算平台计算水平。通过整合目前的分布式机器学习资源, 提供各种类型的数据训练代码模板, 其中, OpenAIChain 官方将通过填写分布式机器模板, 在线监测剩余多少台可用机器, 来作为训练依据。

OpenAIChain 将为 AI 服务提供贡献 SDK 包, Dapp 开发者可以通过调用链上已有的 SDK 包发起 AI 服务, 从而增加应用扩展性。

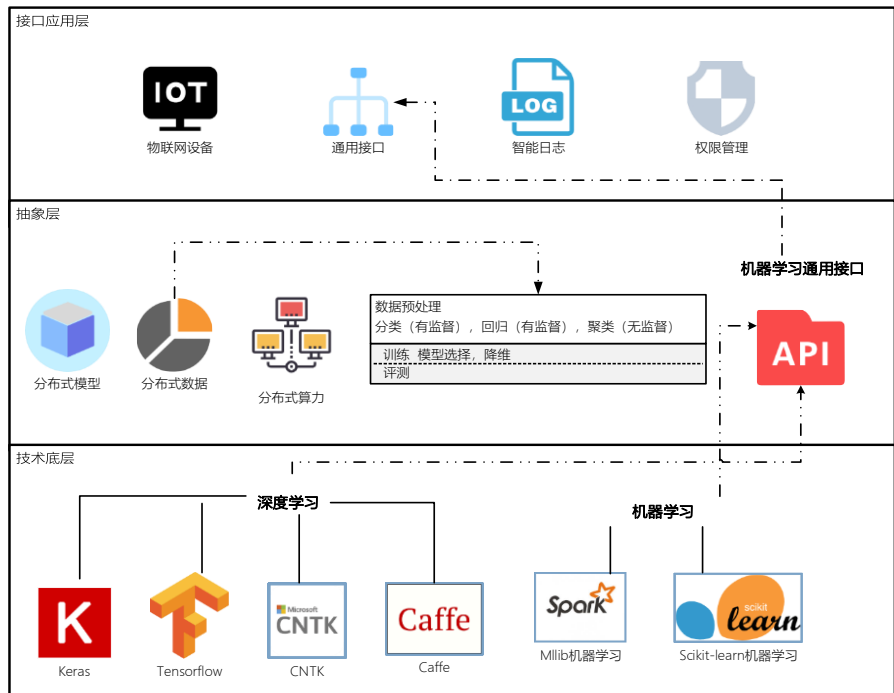


图 4. 合约 AI 接口

2.3.3 合约授权管理

OpenAIChain 合约将提供不同用户访问权限管理模板，Dapp 开发者仅需要调用此 SDK 就可以对合约使用者进行分组权限管理，极大节约开发者开发成本以及提供合约 AES 加密，保证开发者知识产权。

2.3.4 合约资金担保

智能合约（smart contract）在 OpenAIChain 系统中不仅仅起到构建 AI Dapp 的作用，更被用来充当交易的金额担保系统以及模型验证系统。使用系统智能合约，当用户需要获取更多 OpenAIChain 链开发，访问权限甚至使用带宽时，需要更多的 OAC 来获得系统支持，从而避免女巫攻击。OpenAIChain 链中使用智能合约。链上代码往往被称为智能合约，其给人的印象是智能又受法律保护。The DAO 事件使人们看到“智能”合约既不智能，同时没有匹配法律框架，不具有法律效应。OpenAIChain 将对个人开发者知识产权保护，与各地司法部门合作，使链上代码加上特定法律框架支撑。智能合约在 OpenAIChain 中充当了资金担保功能，在用户提交数据、购买代码片、论文训练数据时可通过智能合约资金担保功能保证其代币安全，一旦发现算法欺骗、数据达不到预期可以通过智能合约申请退款业务，以保证用

户资金安全。

2.3.5 合约模型验证

对于数据任务提交环节，节点数据提交完成后，智能合约能调用 OpenAIChain 链上智能验证接口，对数据大小格式进行第一次模型验证，而调用的模型将会随着数据验证次数、验证量增多而变得更加智能，从而节省大量人力用于数据验证。其次，当论文溯源者提交模型至链上，可以通过调用智能合约来对模型数据进行验证，从而缓解网络压力。

2.4 分布式算力与存储机制

算力提供者分为分中心节点以及企业算力提供，分中心节点必须提供一定规模的算力服务，这部分规模的算力服务必须满足两点：

- 论文溯源
- 开发者进行普通开发计算

以上这两点有不同的要求，论文溯源包含足够的服务器以提供论文溯源，一般来说，往链上进行论文溯源较少，OpenAIChain 官方提供在线钱包可以进行模型提交、提供模型参数记录 SDK 以给予模型训练者调用。科研工作者、学生可调用 SDK 来进行模型参数。模型在线训练提交建议在本地已经完成论文修改后，将最后一次训练放置链上再进行标记训练，往往模型训练时间是不确定的，故需要分中心节点提供足够算力。再者，对于模型训练过程过于复杂情况，训练者仅需要通过钱包客户端上传模型至链上记录即可，并讲使用方法以及训练数据记录，以供之后学术复现。

对于开发者进行普通开发，我们提供一套分布式训练 SDK 以及参数记录 SDK，可以对开发者运行模型机记录，开发者付费方式通过占用模型训练占用时间来进行付费计算。OpenAIChain 分中心节点溯源链存储能力有限，无法存下全网所有模型，故每个分中心节点需要利用 IPFS 来完成存储，同样，溯源链关联存储服务器中采用数据模型替换策略，采用最近最常使用（LRU）来保存对应模型，给与模型溯源者一定模型保留时间。

2.5 模型存储和数据隐私保护

2.5.1 模型存储

在构建全局分布式文件系统方面，不同方向已经拥有许多尝试，在学术尝试中，AFS^[12]已经取得成功并至今仍在应用，而学术界外，最成功的系统一直是对等文件共享应用，主要面向大型媒体（音频或视频），其中著名的有 BitTorrent、Napster 及 KazaA，而工业界尝试使用如 HDFS^[13]或者 FastDFS^[14]，OpenAIChain 数据存储层利用点对点内容寻址 IPFS^[15]构建存储服务，在文件被存储发布到 IPFS 后，将生成一个固定哈希地址。将大文件切分为小分块，下载时可从多服务器同时获取，这类型设计很好的适应内容分发网络（CDN），同样可以很好共享各类大型图像、数据流。对于 OpenAIChain 不同节点，将会采取不同策略：

- 全节点常年存储公链交易数据。
- 手机节点采取类似比特币轻钱包模式，仅与全节点进行链通。
- 链上数据使用次数经链上统计，保证数据上传者数据安全不会引起数据丢失。为了帮助模型训练者训练模型，模型者可以将代码放置链上或者模型放至链上并描述清楚模型使用细节，数据的输入输出，放至链上提供模型描述以换取链上代币。

溯源链使用基于 Kademlia 的 dht 算法，条目以 key-value 形式存储在不同节点上，存储规则是中心节点网络中 ID 越靠近 key，条目保存的份数就越多。因此搜索条目的过程也就变成了搜索节点的过程，后续将增加通证规则来保护通证拥有者的应用获得更多的节点连接。全部条目对象组成了有向无环图 DAG 的数据结构。对于 IPFS 加密后数据保密性，OpenAIChain 团队进行自身算法改进确保用户自身数据隐私性。当训练结束后，系统将自动销毁镜像以保证用户代码以及数据不会被泄露。

2.5.2 数据隐私保护

机器学习起源于数据挖掘，同态加密 (homomorphic encryption, HE) 概念是 1978 年 Rivest 等人^[10]提出，允许用户直接对密文进行特定的代数运算变化技术，后来由 Domingo-Ferrer 等人^[11]作进一步改进，基本思想如下：

假设 E_{k1} 和 D_{k2} 分别代表加密和解密函数，明文数据是具有有限集合 $M = \{m_1, m_2, \dots, m_n\}$ ， α 和 β 代表运算，若：

$$\alpha(E_{k_1}(m_1), E_{k_1}(m_2), \dots, E_{k_1}(m_n)) = E_{k_1}(\beta(m_1, m_2, \dots, m_n))$$

成立，则称函数族 $(E_{k_1}, D_{k_2}, \alpha, \beta)$ 为一个加密同态。由于同态加密技术一般基于公钥密码体系，其算法复杂度通常高于其他基于共享密钥加密技术，也高于一般扰乱技术。因此，其不适用于工业化。OpenAIChain 由于提供了分布式 AI 模型训练接口，高校用户模型训练服务，故较关心领域在于保护用户数据或者模型在云端计算中不被他人盗取。对于机器学习模型训练方向，目前来说有三种：

1. 数据加密，模型参数不加密（如医疗影响数据）。
2. 数据不加密，模型参数加密（用户使用公开数据集或是测试自身模型）。
3. 数据以及模型都加密。

针对第三种情况，如果双方的加密算法或者私钥不同，数据无法进行训练。比如 A 提供了一个模型，B 提供了数据，这个时候训练过程就无法进行。

对于数据或者模型参数加密的情况，无法知道损失函数的具体数值，因为最后的残差计算出来也是被加密的。这个时候无法对模型进行评估，无法做交叉验证避免过拟合，无法进行超参调整（比如至关重要的学习率）。所有超参调整必须通过发布者解密后进行确认。

OpenAIChain 使用椭圆曲线加密算法（ECC）来作为公钥密码算法。椭圆曲线算法被广泛应用于数字加密货币领域。例如比特币和以太坊都使用了 secp256k1 签名算法，而 OpenAIChain 选择使用了 ed25519 签名算法。OpenAIChain 钱包地址通过 ECC 算法生成的公私钥对推衍而生成。具体使用比特币的 BIP173 协议中提出的编码算法。该算法是一个针对原有比特币 base58^[3] 地址编码算法基础上的一个改进版本。ed25519 算法相对于 secp256k1 更加高效，同时安全性也非常高。目前也被广泛应用很多加密数字货币项目中，著名的项目例如 Zcash、公证通（Factom）、新经币（NEM）等，以太坊的创始人 Vitalik 也曾在博客中公开表示，以太坊计划在新版本中切换到 ed25519。ed25519 的好处是在不损失安全级别的情况下，显著提升运算效率，其效率是 secp256k1 的很多倍。以 ed25519 的论文中的实验为例，该算法完成一次签名需要 87548 个 CPU 循环，一个 4 核 2.4GHz 的 CPU 每秒可以完成 109000 次签名。密钥的生成也非常高效。而 ed25519 的安全级别和 secp256k1 的级别相同，且都是 128 位的安全级别。基于 ed25519 可有效防止量子计算机攻击。

2.6 基础服务及开发工具

目前各种公有区块链的开发者工具不够完善，对于多语言跨平台支持性极低。OpenAIChain 开发组将依据底层虚拟机完善各种编程语言支持，提供 AI 服务特点，提供链上数据所训练的模型调用、兼容各大厂商人工智能接口，以及开发独立区块浏览器，整合流行 IDE 完善插件支持（包括 Eclipse, JetBrains, Visual Studio, Atom 等），智能合约形式化验证工具，以及移动端 SDK 等。

3. 关键技术

3.1 OpenAI Rank 指数

OpenAIChain 需要一个价值尺度来衡量数据、模型算法贡献者所给予的分享，我们提出 OpenAI Rank 来 OAR (OpenAI Rank, 开放 AI 服务指数)，类似于 Google 的 PageRank^[24]，用来衡量数据、模型的高维信息。OAR 综合考虑模型购买流动性、资金传播速度、广度以及账户活跃程度，真正给社区进行数据分析统计，OAR 可用于搜索、推荐、广告等领域。

3.1.1 指数总设计

我们对每个账户、数据、模型重要程度量化为 OAR 指标形式。OAR 有下面三重描述：

- 易用性，数据、算法或者模型是否对用户足够友好，让足够通俗易懂；
- 流动性，即一个数据集、算法被使用次数、交易频率和规模量度；
- 可信性，以上两点均必须考虑可信，只有可信了链上智能才能成立；

下面章节中我们将设计 OpenAI Rank 基本框架。

3.1.2 排名算法

- 数据排名算法：通过企业购买使用、个人用户调用情况，进行排名算法计算（待补充）

这里我们将设计一种 OAR 中包含了用户的 AttentionRank（注意力）推荐（待补充）

- 算法问答排名算法：某个问题被浏览次数越多，说明这个算法开发问题越受关注，得

分越高，

$$OAR = \frac{\lambda(\log_x Q_{Views}) + \frac{Q_{Answers} \times Q_{Score}}{\gamma} + Sum(A_{Recommend})}{((Q_{age} + 1) - (\frac{Q_a - Q_{update}}{2}))^{1.5}}$$

其中， Q_{score} 为问题得分等于赞成票与反对票之间的差值，问题越受好评，排名越靠前。

$\lambda \log_x(Q_{Views})$ 是问题被浏览次数， x 与 λ 控制得分函数变化， $Q_{answers}$ 为问题的数量，代表问题参与的回答人数， γ 为 OpenAIChain 调整参数， $A_{Recommend}$ 为社区问题 Follow 数以及问题大 V 推荐， Q_{age} 为问题发表时间，单位为秒，若一个问题存在时间越久，距离上次回答时间越久， Q_{age} 以及 Q_{update} 这两个值将会增大，致使总得分越小。

· 文章排序分享贴：对于 AI 知识帖子分享，需要一个价值尺度衡量文章更新频率以及用户推送，类似于 Reddit 投票算法，OpenAI 官方对于任何一个时刻 t_0 ，记录时间 $[t_0 - T, t_0]$ （ T 为某领域帖子创建初始时间），所有帖子的点赞数或否决数，其中，每篇帖子的得分如下：

$$Score = \log_{10} z + \frac{yt}{S_r} + \lambda R$$

z 是一篇知识（算法）分享贴表决质量（也就是受推荐质量）， z 取决于 x ， x 为帖子赞成票与反对票之间差值。 y 为投票方向， S_r 为官方指定更新帖子时间， λ 为社区活跃度粉丝占比指数， R 为板块帖子收社区最活跃份子赞同数目，数分别对应如下：

$$y = \begin{cases} 1 & (x > 0) \\ 0 & (x = 0) \\ -1 & (x < 0) \end{cases} \quad z = \begin{cases} |x|, & x \neq 0 \\ 1, & x = 0 \end{cases}$$

3.1.3 抗操纵能力

知识分享不是仅仅靠站内人气就可完成，更是要更多站外人认可，在知识贴分享过程中，我们会统计文章浏览量以及评论，由于文章浏览仍以 HTTP 形式与用户互动，仍有可能遭受恶意流量注入，OpenAIChan 将会在服务器部署 HTTPS 以及内容安全策略（CSP）以提供一个白名单机制，限制白名单内指定 URL，以此屏蔽广告以及流量注入。

3.2 激励机制

3.2.1 奖励及分配算法

对于用户层面，OpenAIChain 将采用排名算法进行统计后对每个数据提供者、用户以人气热度来提供，用户本身持有 OAC 就是对 OpenAI 社区的有力支持，并且 OAC 价格越高，那么系统每日用来奖励优质内容的总价值越高，从而激励数据、算法上传。

对于分中心节点层面，详见 3.2.2 描述。

3.2.2 分中心节点激励机制

分中心节点将起到论文溯源、流量转发机制，分中心节点将面对巨大的流量压力，负责出块以及地区的论文溯源记录提交，分中心节点激励机制每年可以获取 OpenAIChain 官方收益及设备投资。但是参与分中心节点竞选必须是符合以下打分规则。

- 全球学校、公司信息以及科研实力；
- 测试节点服务器类型、服务器配置、硬件扩容计划；
- 团队价值观，社区计划及资金使用透明度；
- 预算超支以及技术解决方案；
- 公共网站以及在 OpenAIChain 上的社交账号；

对于国内高校用户，一旦参与竞选 OpenAIChain 节点成功，OpenAIChain 将会大力支持国内院校发展，为国内院校提供一定数量服务器设备以及进行投资，希望为国内尽可能培养 AI 方面人才，且对国内节点激励将会兑换成对应人民币来支持国内节点算力提供。其中对于全球分中心节点，每年将会增发 5% 的 OAC，其中 2% 用于节点激励，3% 用于后续发展，为分中心节点购入一定规模设备。

3.2.3 全网节点激励机制

要了解全网节点激励机制就必须清楚全网节点如何得到奖励，OpenAIChain 平台通过用户提交数据、代码片、模型来获取 OAT 代币奖励，关于各个过程入下所描述，

一、数据采集，OpenAIChain 平台定期发布 AI 数据采集奖励活动，采集的数据方式有以下来源：

OpenAIChain 链致力打造共享人工智能平台

- 官方平台发布数据收集任务：官方平台根据各个 AI 行业数据缺失特点，定期向平台用户发布数据采集任务，任务采集不限于语音数据、图像数据、文本数据等，平台用户需按照采集说明完成并提交数据即可获得相应数量代币；

- 企业公司可通过支付一定量代币来收集数据，其中支付金额 95% 归数据提交用户，而 5% 金额用于 OpenAIChain 设备维护，这一部分数据所有权归企业所有；

- 学术公开数据集奖励，上传者需附带学术公开数据集下载链接以及说明数据集使用方式，获取学术数据回报奖励，这一部分数据供下载者免费使用；

二、模型、代码提交，学术用户、开发者甚至企业可以提交自己的学术项目、代码到 OpenAI 链上，得到丰厚知识分享奖励，这部分将是促进开发者、高校学生交流的重点；

三、知识分享奖励，知识本身外部性分享程度越高，越能展现知识网络效应，OpenAIChain 根据用户在 OpenAIChain 知识问答平台以及博客分享平台上收获点赞数、阅读数来对开发者进行奖励。

3.2.4 验证节点激励机制

只有在 OpenAIChain 上掌握足够的权益才能够成为验证节点，未成为验证节点的其他节点称为普通节点。这部分权益指上传个人真实资料，表明行业从业资格。例如，医疗从业者需上传从业资格证以及个人档案，通过审核后，方可成为数据验证节点。验证节点在完成数据校验任务后将获得数据上传节点的 2 倍收入，一旦发现可疑数据，与之对应的数据上传普通节点也会承担相应损失，同时也激励全网节点将所掌握权益委托给可信的验证节点，从而提高 OpenAIChain 数据采集真实性，这一准则同样适用于算法上传验证节点。

3.3 区块链搜索引擎

3.3.1 搜索基础架构

随着越来越多的数据被用户提交、算法分享贴被上传、智能合约被部署，用户面对海量的信息，搜索的需求也变得突出起来。我们将用多种手段为各种资料建立合适的索引：

- 为数据、算法上传建立规范，任何符合此规特定类型数据，都能被检索并被用户搜索到，建立链上应用商代，规定开发者在创建算法仓库时，提供详细信息描述。

- 建立智能互联 App，供安卓、苹果用户下载，建立关联微信小程序，方便用户上传数

据，建立方便快捷使用的互联 App 往往是最能吸引用户的最重要方式。

- 爬取智能合约相关 DApp，为其和区块链智能合约建立映射关系；

3.3.2 关键词搜索

用户提供关键词，描述智能合约的标题、作者、功能等文本信息，在海量的智能合约中找到匹配的合约。对于文本搜索，目前有非常成熟的算法和技术，基于自然语言处理和倒排索引技术，我们可以在海量的代码、模型索引库里高效的检索和排序。关键的技术如下：

- 面向主题的分布式爬虫技术；
- 多语言分词技术：对于西文词汇，分词较为简单。对于中文分词，有多种算法可进行分词：正向最大匹配，逆向最大匹配，最短路径分词，统计分词等；
- 查询词纠错、语义理解；
- 倒排索引，分布式搜索架构；
- 排序算法，将搜索结果排序；

其中排序算法结合 OpenAI Rank 来设计，我们把区块链世界中用户之间的转账类比互联网世界的网页引用关系，构建出去区块链交易图。

3.3.3 模型算法搜索

OpenAIChain 开发组将实现一个搜索服务，实时检索所有智能合约，做多语言的分词，建立全文索引，最终提供一个友好的 Web 界面给用户使用。OpenAIChain 提供排名算法的公正性和每个节点的可验证性保证了中心化搜索服务的公正性，搜索后台代码都将开源给社区。我们将用多种手段为智能合约建立合适的索引：

- 爬取 AI 技术相关网页资料，为其和 AI 应用建立映射关系；
 - 鼓励开发者上传验证过的机器学习代码，分析其代码功能和语义，为源代码建立索引，提供相似代码搜索；
 - 为分布式代码训练建立规范，任何符合此规范代码，都能被检索并被开发者搜索到；
- 传统搜索引擎资源获取部分使用的是盲目式遍历算法，即对所获得链接进行遍历，抽取相关信息保存，抽取相关信息后供搜索引擎调用。

3.3.4 趋势榜单

OpenAIChain 链将结合 OpenAI 指数构建趋势榜单，提供给用户可视化的区块链多维度价值。

- **数据贡献者榜单** 根据数据提交数量、质量计算数据贡献者榜单，以及数据贡献度快速提升榜单，奖励数据提交者；

- **知识贡献者榜单** 根据文章、算法分享量，订阅量以及点赞数奖励社区知识贡献者，同时设置知识贡献度快速提升榜单，有偿激励知识分享者；

3.4 GPU，CPU 分布式训练

OpenAIChain 中同样支持企业、高校将多余算力、硬盘贡献出来，以此换取代币。当前分布式并行计算节点可以配置多核 CPU 和多个显卡构建节点内多 CPU 多 GPU 并行计算系统。系统内每个计算单元都具有强大计算能力，充分发挥节点内多 CPU 和多 GPU 协同计算性能，既是提高单机模型训练效率有效途径，又是构建大规模复杂场景高效分布式并行计算系统的重要基础。训练时分两种并行化：模型并行化（model parallelism）分布式系统中的不同机器负责单个网络模型的不同部分，如神经网络模型不同网络层被分配到不同机器中；数据并行化（data parallelism），通常作为分布式系统首选。不同的机器有同一个模型的多个副本，每个机器分配到数据的一部分，然后将所有机器的计算结果按照某种方式合并。两种训练方法并不互斥。假设一个多 GPU 集群系统，可以在同一台机器上采用模型并行化（在 GPU 之间切分模型），在机器之间采用数据并行化。主要方法差异在于参数平均间工作节点与参数服务器之间更新信息的传递。

OpenAIChain 数据并行化式的分布式训练在每个工作节点上都存储一个模型的备份，对每个节点的 minibatch 而言，参数平均通常有一个大于 1 的平均周期（averaging period）在各台计算机器上处理数据集的不同部分，后在各节点之间同步模型参数，以 GPU 来说，模型参数分为同步式和异步式两种。

- **同步式算法**：标准同步式算法每次迭代式 $w_{t+1} = w_t - \alpha \times \frac{1}{n} \sum \Delta w$ 为标准，先从参数服务器（Parameter Server, PS）中把模型参数 w 拉取（pull）到本地，后使用新的模型参数 w_n 计算本地 minibatch 的梯度 Δw ，最后将计算出的梯度 Δw 推送（push）到 PS。PS 需要收集

所有节点梯度，后根据 w_{t+1} 进行平均处理更新模型参数，其中 α 为学习率，若用户代码调用基于 Spark 平台的深度学习包 CaffeOnSpark 则采用同步式算法，计算集群算法如下图所示：

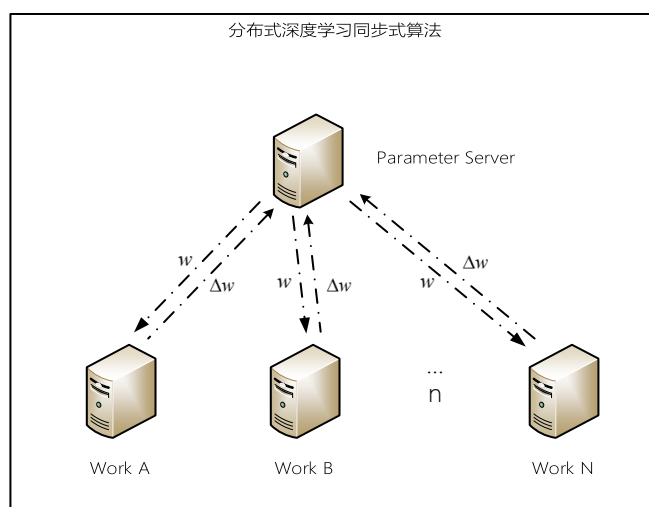


图 5.同步式算法图

上述这种强同步式算法，会由于系统中各个机器之间的性能差异，导致所有的节点都要等待计算最慢的一个节点执行完，产生木桶效应，通讯时间会造成同步扩展瓶颈。

·异步式算法：异步随机梯度下降算法 (Asynchronous Stochastic Gradient Descent, ASGD) 是对同步式算法的改。PS 仅需收到一个节点的梯度值就进行更新，消除木桶效应并利用梯度的延迟更新，大幅度减少网络通讯延迟造成时间开销，但会造成梯度值不稳定，导致模型训练准确率下降。目前解决异步随机梯度下降方法中梯度过时所造成的影响主要有对每次更新的梯度 Δw ，引入缩放因子控制梯度过时对全局影响，以及采用弱同步^[25]策略，第一种参数更新形式为： $w_{i+1} = w_i - \lambda \alpha \Delta w_i$ ，弱同步策略相对于立即更新全局参数向量，参数服务器等待手机 $n(1 \leq j \leq n)$ 个节点产生的 $s(1 \leq s \leq m)$ 次更新后，按 $w_{i+1} = w_i - \frac{1}{n} \sum_{j=1}^s \lambda \Delta w_j$ 。

主流分布式深度学习框架，如 MXNet、TensorFlow 都采用异步随机梯度下降算法及其变种。OpenAIChain 将会提供全套在线的分布式模型训练视频，让开发者学习调用，通过整合 Tensorflow、Spark 等分布式深度学习代码，提供一套分布式模型训练模板，让开发者可以轻松调用可使用的有效算力服务器。

3.5 分中心节点溯源链

分中心节点提供计算任务分发、区块生成、论文溯源功能，而在论文训练完成后，或者

OpenAIChain 链致力打造共享人工智能平台

数据提交，而溯源链是每个分中心节点必须开启，用于学术论文溯源。

目前区块链技术中主要有三种跨链技术：公证人机制（Notary schemes）、侧链/中继（Sidechains/relays）、哈希锁定（Hash-locking）。公证人模式是通过引入一个中介机构来建立双方信任，提供一个被称为“连接者”的第三方中心化加密托管机构，通过机构帮助资产在不同链间传递。侧链/中继模式是通过中间链来担任不同区块链间的通道，在主链上用多重签名来锁定资产，在侧链上锚定，通过共同投票决定交易是否有效。最后哈希锁定常见于闪电网络等通过创建支付通道来完成资产交换。OpenAIChain 在溯源链与主链之间采用“公证人机制+侧链”混合技术来实现跨链价值通信，但通信的内容仅仅是区块头之间的提交，以最简单的实现方式来说，采用 Keyber Network 所提出的 peacerelay 机制，建立简单智能合约的跨链通信，但在数据写入环节会花费代币，数据写入时 OpenAIChain 会在分发给这个第三方中心化可信机构 Paper Token，Paper Token 为论文溯源链向 OpenAIChain 主链提交区块头所花费代币，这个代币建立在 OpenAIChain 网络定义的论文溯源协议（Paper Traceability Protocol, PTP）网络中。

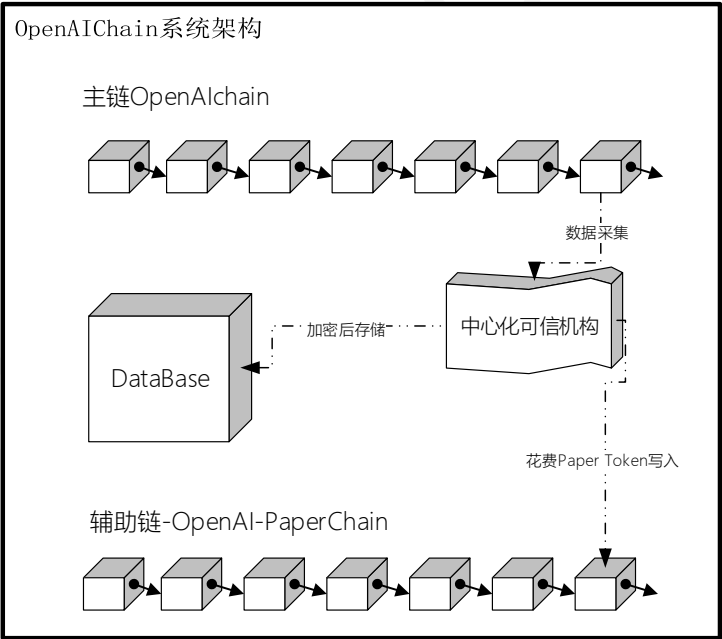


图 6.分中心节点溯源链

OpenAIChain 中论文链将在初期会采取公证人模式，在 OpenAIChain-PaperChain 与 OpenAIChain 主链交互中，于 OpenAIChain 主链上部署一个智能合约用于读取论文链区块头。论文代码提交记录于论文链中，其中涉及 Dapp 记录于主链产生 Token 记录费用问题，官方会在论文链上发布新代币 PaperToken 用于论文溯源，PaperToken 仅用于记录而不用于出售，使用时，对 PaperToken 代币与 OAC 进行双向锚定。

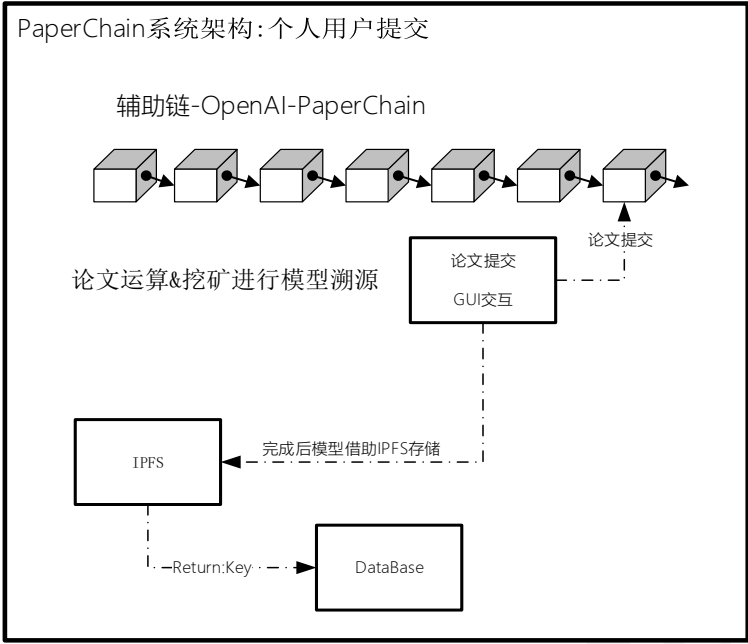


图 7.用户提交代码至 PaperChain

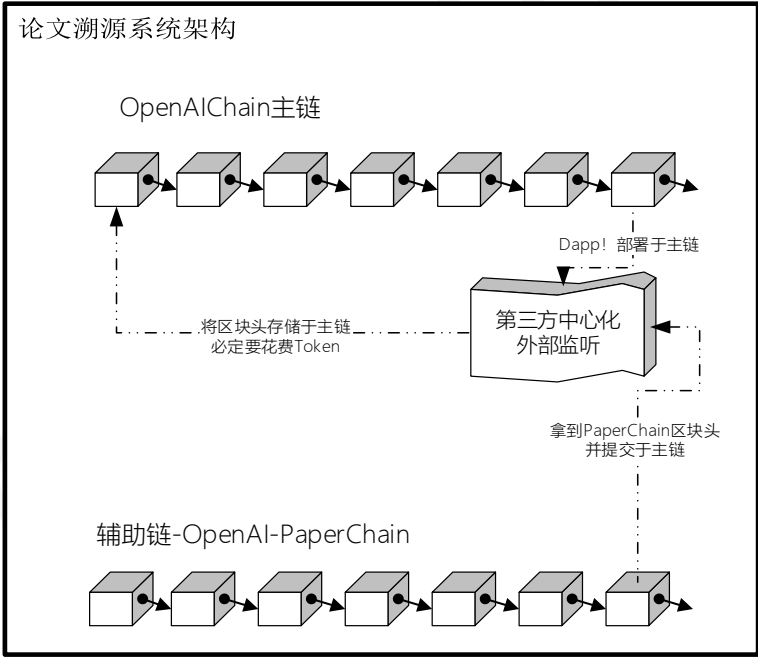


图 8.论文溯源代币产生及销毁

3.6 智能合约升级设计

3.6.1 合约调用 AI 即服务

OpenAIChain 智能矩阵旨在提供一个基于共识的、分布式的、虚拟的 AIaaS 云基础设施，

OpenAIChain 链致力打造共享人工智能平台

借助区块链经济系统，调用全球 AI/机器人技术力量，构建世界人工智能。可以调用语音识别，人脸识别，手写识别等等系列的人工智能接口与应用。

3.6.2 合约抗风险能力

目前以太坊智能合约的设计是代码一经部署，不可变化，代码逻辑从部署的时刻起，便永远不再具有升级的能力，学术界会议上，较为关注智能合约漏洞以及形式化验证（基于数学描述系统性质，期望利用数学分析以提高设计可靠性和鲁棒性）。以太坊上的智能合约可升级方案大体上分为两类：对外公开代理合约 (ProxyContract) 以及合约的代码和存储分离，第一类代码结构简单，并将请求转发至功能合约。第二类是把合约的代码和存储分离，存储合约负责提供方法，供外部合约读写内部状态，代码合约做真正的业务逻辑，升级时只需要部署新的代码合约，不丢失所有的状态。这两类方案都有其局限性，不能解决所有问题：合约的代码和存储分离在设计上增加了很多复杂度，有时候甚至不可行；代理合约虽然能够指向新合约，但是老合约的状态数据并不能迁移；有些合约在开始开发时，没有良好的设计，没有为以后的升级留下接口。近年来，模型驱动 (model-driven) 的设计方案逐步被工业界重视并认为是可行方案，该方法将模型作为整个系统开发过程核心元素，在设计阶段就简历系统体系架构模型，在设计初期就简历系统体系结构模型，尽早进行验证分析。同时，尽可能模型重用以及基于模型转换的自动或半自动需求过程都有助于降低系统开发时间和成本。结合 OpenAIChain 自身系统的软/硬件结构、运行时环境、功能行为以及非功能属性等，OpenAIChain 将 OpenZeppelin 推荐为建立安全智能合约标准，如，合约建立若涉及交易转账时应将合约推迟付款功能，增强代码复用性等提高智能合约抗风险能力。

4. OpenAIChain 生态驱动

4.1 面向全人类--数据激励驱动平台

OpenAIChain 致力于打造面向全人类数据驱动平台，如图 1 所示。

OpenAIChain 链致力打造共享人工智能平台

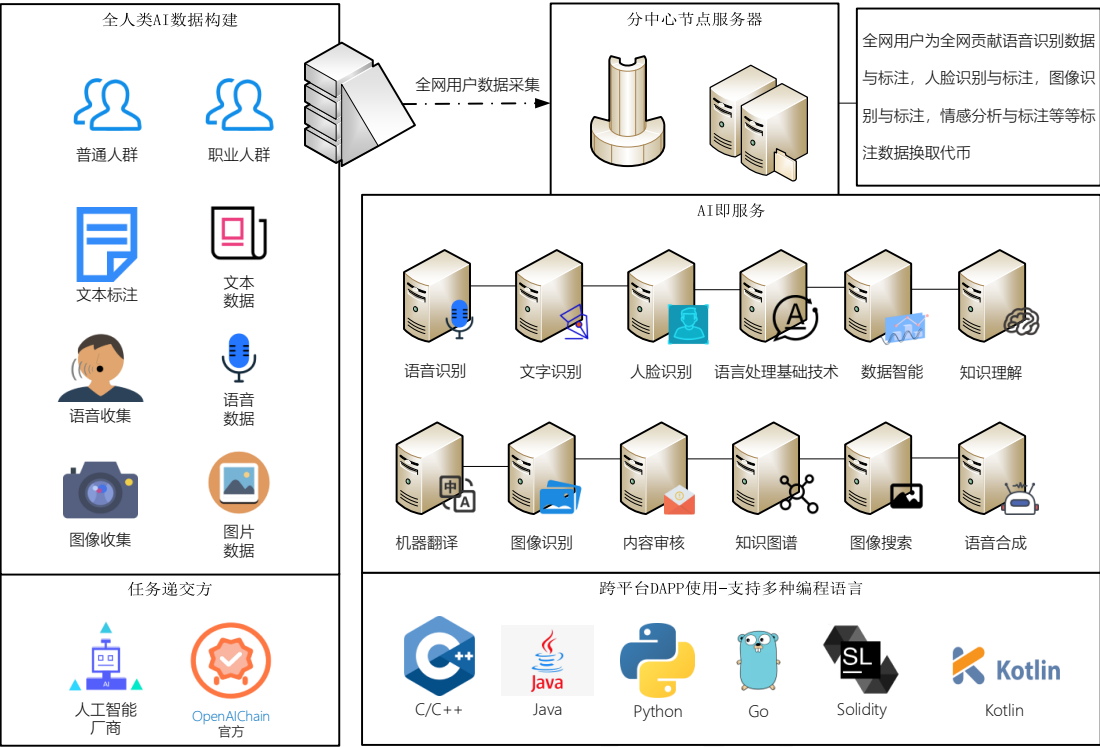


图 9.OpenAIChain 数据驱动生态

OpenAIChain 通过对人工智能全生态的各个环节进行梳理，将各参与者的资源和需求进一步细化，从而更好的刻画参与者之间的协作关系，促进整个生态的合作共赢，推动人工智能的快速发展。

对普通用户而言，制造有偿数据购买服务，OpenAIChain 搭建数据有偿交换发布机器学习任务，让全名参与公共数据采集及标注。如，场景一、语音识别标注数据采集：

OpenAIChain 自身平台或者是人工智能厂商借助 OpenAIChain 平台发布语音数据采集任务，全网用户参与进入数据采集任务并获得代币，数据归属权由任务发布方所有。若是 OpenAIChain 官方的任务，则全网所有用户将获得使用权，开发者通过支付少量代币可对数据进行调用。

OpenAIChain 链致力打造共享人工智能平台

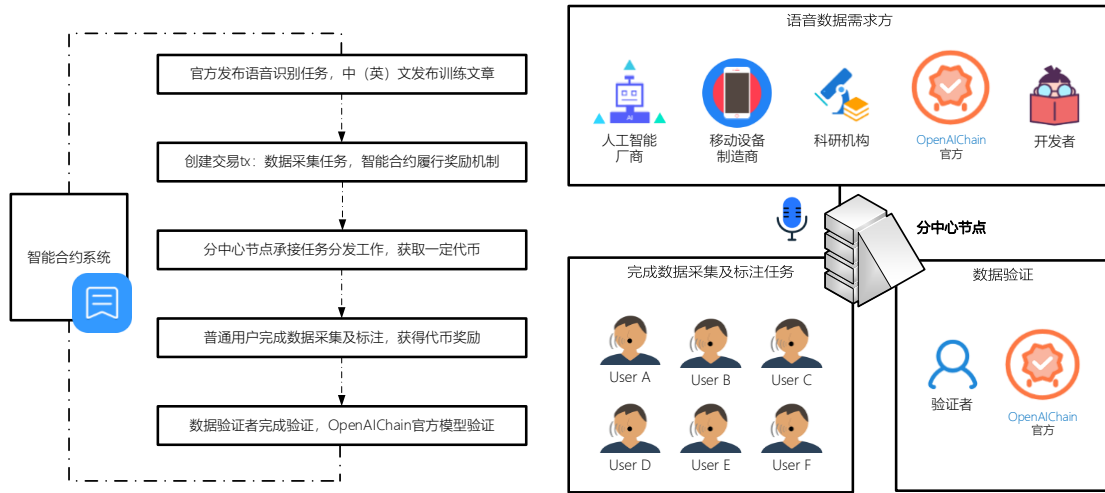


图 10.语音标注任务

场景二、图像标注数据采集

OpenAIChain 官方、特定数据需求方如企业、科研机构等将特定数据表述，发布任务到 OpenAIChain 任务发布平台，摄像用户通过路上拍照、并对特定物品如车辆、车牌等图像标注赚取代币。汽车厂商等亦可收集更多的道路标注信息，交警可获取道路车辆信息，构建信息化社会服务；再者，退休的医学从业者可通过自身专业知识在 OpenAIChain 平台大量标注医学影像数据，不仅仅增加自身收入，同时也为医学人工智能厂商提供更好的图像数据服务。OpenAIChain 通过互惠互利的区块链有偿奖励机制构建 AI 生态。

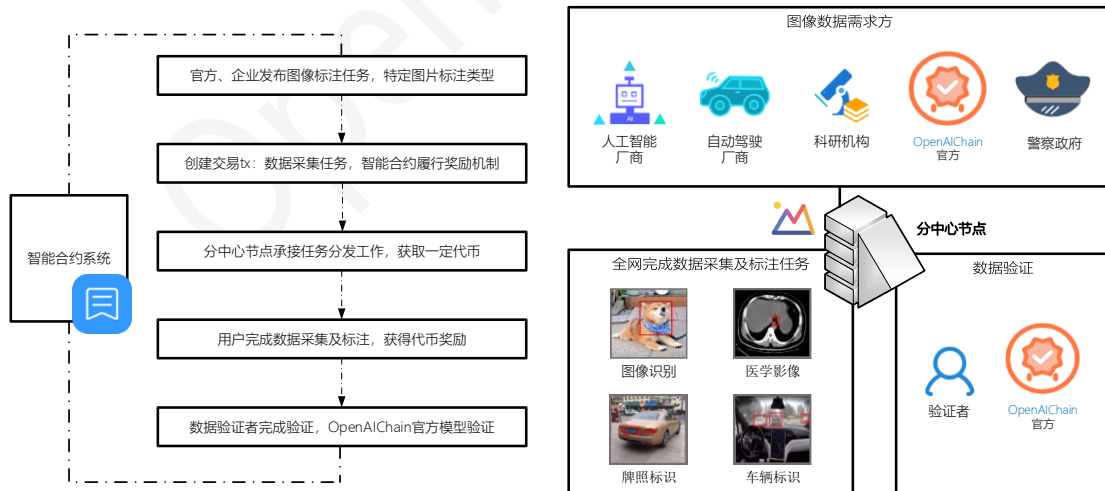


图 11.图像标注任务

场景三、文本标注数据采集

文本数据标注是一个庞大任务，对于文本标注，情感标注，往往在不同语言环境下表述不同，这需要大量人力来判断。OpenAIChain 这种全民参与数据标注奖励机制能快速帮助移

OpenAIChain 链致力打造共享人工智能平台

动设备制造商获得有标注文本信息，同时，OpenAIChain 针对目前知识图谱领域数据源少问题，将文本实体通过标注后作为验证图谱信息，供各大高校、学生作为公开数据集使用。

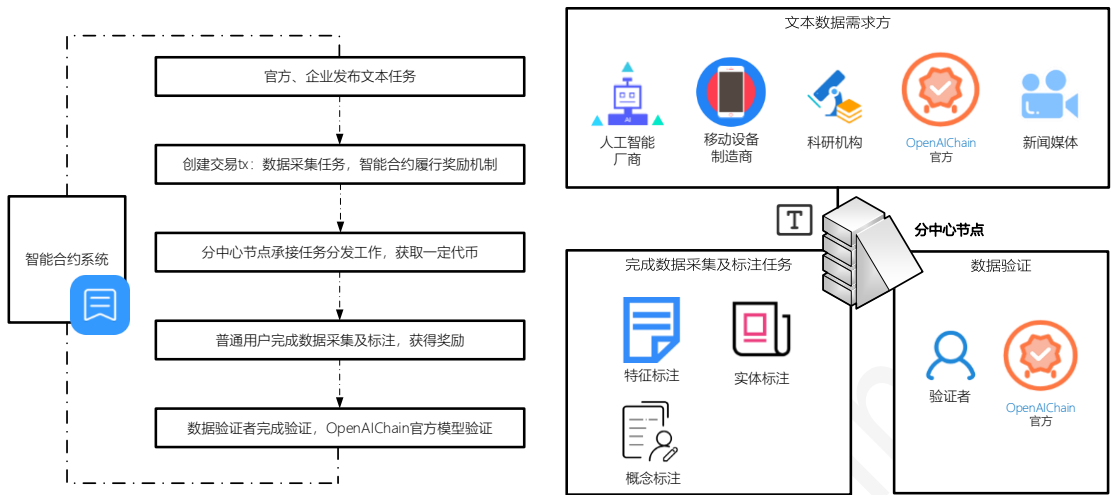


图 12.文本标注任务



图 13.OpenAIChain 手机客户端将收到任务推送

4.2 面向学习者--知识分享平台

OpenAIChain 将依托区块链底层构架，连接数据资源方、应用开发者等角色，有效组织生产力和生产要素相匹配，并通过内生的激励机制吸引更多的资源所有者参与，逐渐丰富数据储备和应用场景，从而实现系统的良性循环，创造更大的价值。

OpenAIChain 链将推出 AI 搜索引擎、社区交流问答以及有偿付费机制，提供公开的资源信息发布渠道，以解决 AI 引用的开发流程所需要资源流转问题，提高 AI 开发资源层面的协作效率。

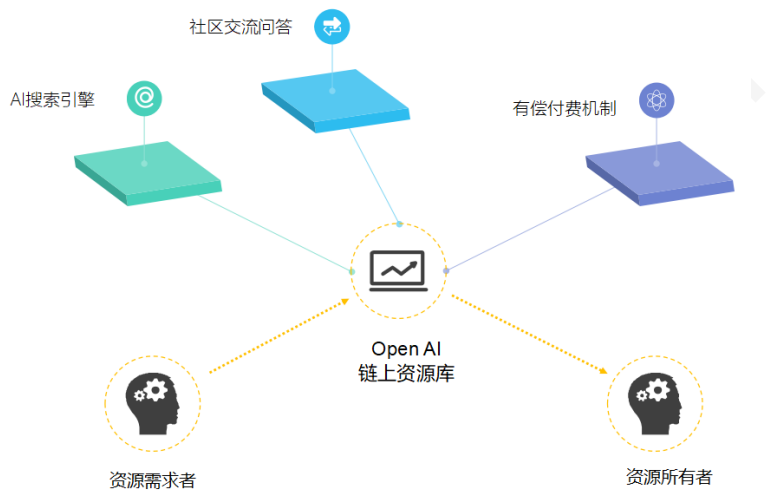


图 14.OpenAIChain 链构建基于区块链的 AI 届交流社区及开放代码仓库

OpenAIChain 打造公开透明的去中心化资源交易平台，AI 开发所需的各类资源可以在链上交易，资源需求者向资源提供者支付 OpenAIChain Coin (OAC)，即可获得资源使用权限。随着市场上越来越多的资源引进，将逐步实现市场化的公允定价，从而促进 AI 应用开发的规模化发展，让人工智能可以更快、更好、更安全地惠及每个人的生活。同时，OpenAIChain 链打造知识有偿社区，让 AI 模型训练者能快速寻找到数据解决之道。

OpenAIChain 链致力于打造共享人工智能平台

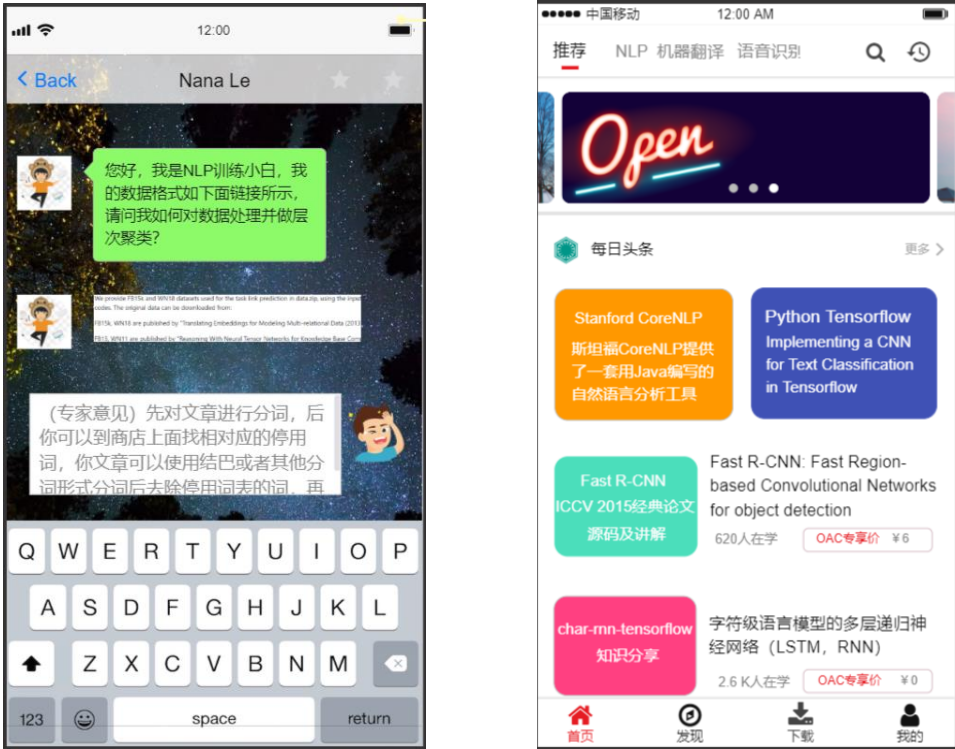


图 15.OpenAIChainAI 知识分享平台以及有偿知识问答

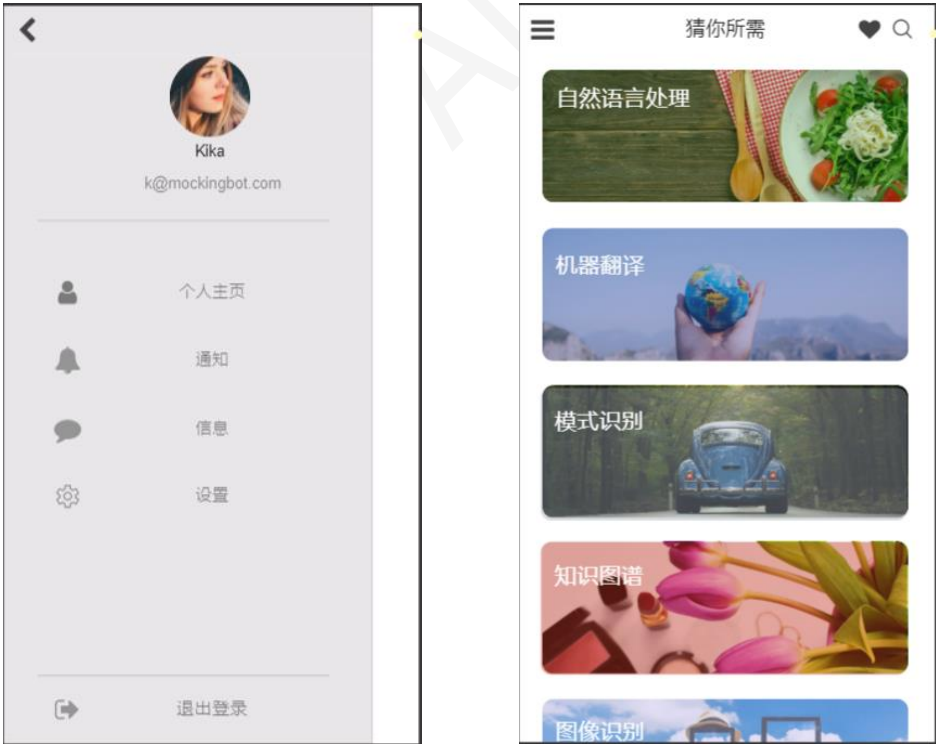


图 16.OpenAIChain 链上个人 AI 搜索引擎

OpenAIChain 链致力打造共享人工智能平台

4.3 面向高校及科研工作者--资源协作平台

高校以及科研工作者可以调用 OpenAIChain 所提供数据资源、验证论文模型、AI 视频教学资源以及调用各大厂商的 AI 服务。高校间不同学科可进行互相互动，如环境科学领域可与计算机学科在空气污染指数分析建立联系。



图 17.面向高校资源协作平台

4.4 面向多领域--打造区块链切实落地项目

4.4.1 配合教育领域打造区块链机器学习应用落地项目

AI 是未来各国的利器，培养人才需从小开始，OpenAIChain 提供链上教育平台，配合中国政府切实打造区块链落地项目。OpenAIChain 将与合作地区中小学完成学生信息记录，利用自主研发成绩智能分析工具重点分析各个学生情况，精准分析学生轨迹，快速提高学生成绩。同时，配合各地政府打造 AI 领域人才，进行链上视频教程，从而有效避免自主产权丢失，数据记录被抓取。

OpenAIChain 链致力打造共享人工智能平台

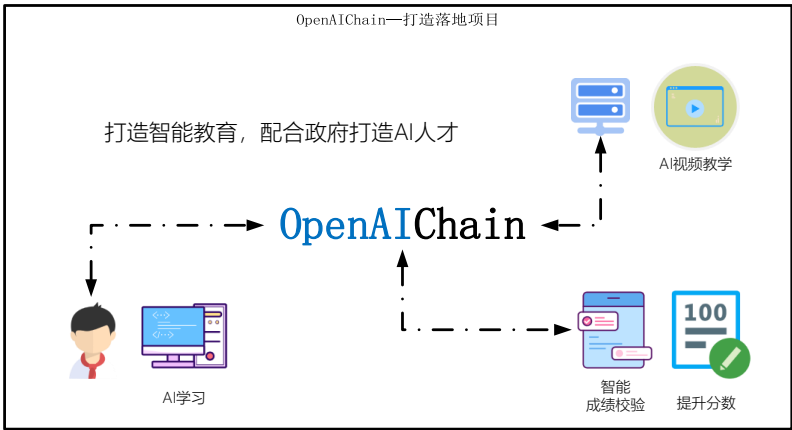


图 18.配合政府打造教育落地项目

4.4.2 学术工程溯源打造标准

如图 7 所示，OpenAIChain 将打造公平公正的学术溯源标准，这里高校、科研机构都是通过系统控制器，通过创建一个交易部署到 OpenAIChain 区块链上，数据、代码一经部署就会保存到备份系统中，以保证代码安全。而上传的数据与代码同样会通过分中心节点进行计算服务，实验完成后代码、数据将记录到溯源链上。

期刊、会议可根据实验者实验记录 ID 号在 OpenAIChain 中找到相对应的实验记录，并且可以通过论文提交者授权密钥解锁并下载代码、数据。若论文提交者拒绝将项目开源，则期刊、会议可通过 OpenAIChain 智能合约系统所提供的验证接口来对论文递交者的模型进行验证。同时，OpenAIChain 将收集全网公开数据集，为计算机学科领域提供快速访问数据链接。

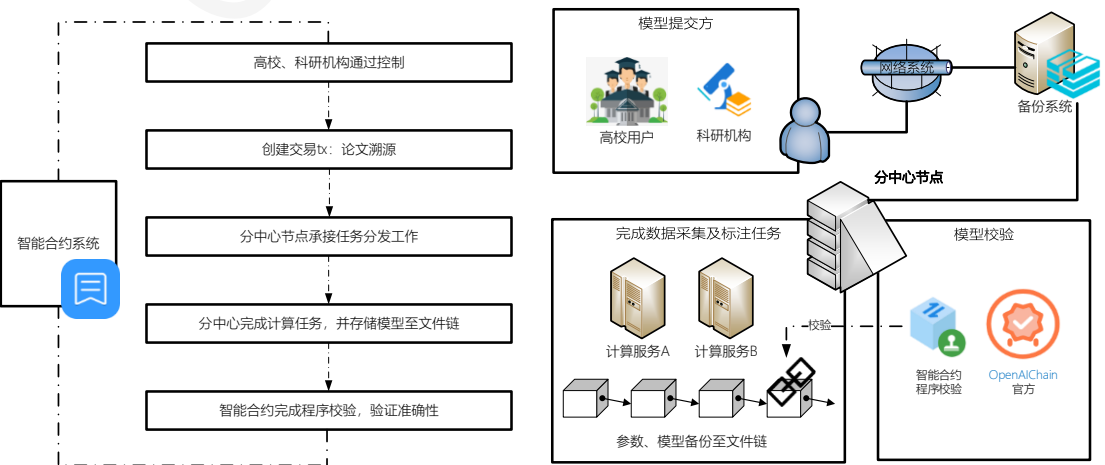


图 19.学术工程溯源平台，打造公平公正标准

4.4.3 智能人才招聘

目前的招聘过程往往需要第三方平台协助进行撮合,而这些平台则掌握了大量的求职者真实信息。对于求职者而言面临严重的私人信息泄露的风险,随之而来的电话、邮件骚扰也让人不胜其烦。

未来,公司或个人可以通过 OpenAIChain 上的个人代码提交记录、知识分享次数寻找各 AI 领域适合人选。

未来,公司或个人可以通过 OpenAIChain链上的 AI 应用商店,找到 AI 智能招聘应用:

- 1.在匿名化的区块链系统中,个人的代码提交、社区贡献将会记录在链上,系统会对活跃度达到等级用户开放简历权限,企业对应的AI板块寻找人才;
- 2.智能招聘应用将通过算法对双方进行匹配,并将匹配信息反馈;
- 3.若企业有意向,则开放简历投递入口,花费少量代币获取个人简历;
- 4.同时若求职者有意向应聘,则可以进行链上身份认证并将简历发送到该企业;

无论企业还是个人使用者,只需到 AI 应用商店中选择相关应用,向开发者支付 OAC,就可以用自己的资源创建个性化的智能招聘流程。这将大大提升招聘效率,并避免第三方平台存储大量私人信息而产生的风险。

4.4.4 算法竞赛服务

OpenAIChain 官方、企业可以上传自身数据设置算法竞赛供 AI 企业选择适合方向人才,增加全民算法 AI 算法互动。成为全球的人工智能竞赛平台。根据智能合约的 AI 接口,算法与模型计算识别率进行自动排名。

4.5 面向企业用户--打造贡献算力存储平台

OpenAIChain 链公链上线后,OpenAIChain 社区会为中小型企业,学校用户打造可以训练模型的算力,同时,为中小型企业打造低成本问题人工智能厂商硬件投入机制。通过将挖矿算力转换为机器学习或深度学习算力,若将模型部署到 OpenAIChain 平台进行训练,人工智能企业可以降低 70% 的硬件成本。

人工智能产品需要通过神经网络来计算训练模型,而数据模型训练过程需要消耗大量的计算资源,考虑到大多学校用户情况,大多数深度学习用户缺乏有效设备训练模型情况,

OpenAIChain 链致力打造共享人工智能平台

OpenAIChain 解决了目前阶段大多数学校没有大量资金购置 GPU、FPGA 等硬件资源，这些对于大部分中小型学校来说，都是巨大的负担。OpenAIChain 中挖矿节点收入来源主要由训练支付费用和挖矿代币组成。其中训练支付费用是针对中小型企业、学校用户购买基础神经网络计算资源的费用，其交易代币为 OAC，并根据智能合约设计奖励系统对挖矿节点进行激励。学校用户往往提交次数多，算力消耗小，对此，OpenAIChain 给予教育用户一定优惠以及激励，鼓励更多校园用户参与 AI 方向学习，从而推动 AI 行业发展。

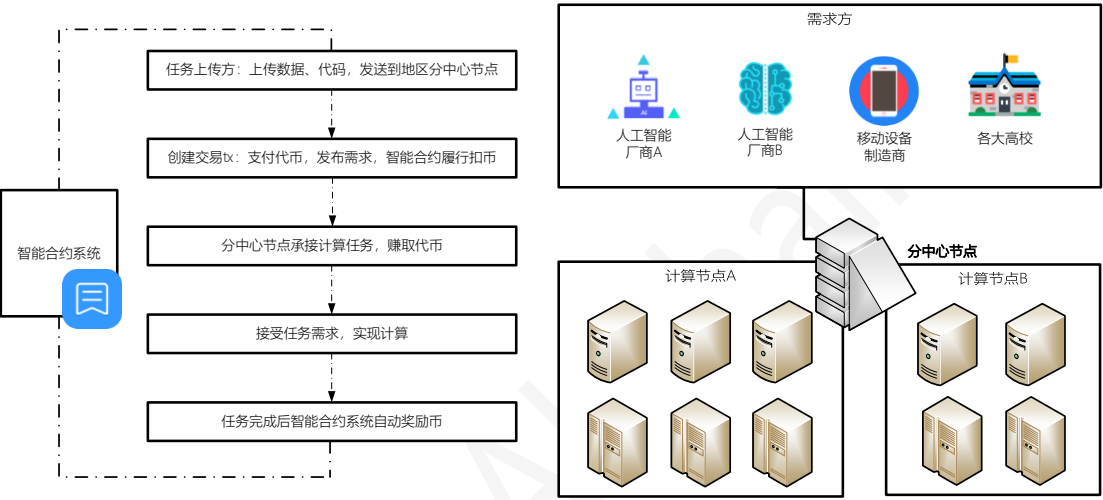


图 20.面向高校资源协作平台

4.6 面向开发者--资源整合平台

OpenAIChain 整合 tensorflow、CNTK 等资源，提供分布式模型机制，让开发者能快速获取相应的标注数据集、算法、论文。同时面向无足够算力的开发者，提供 AI 接口服务，让用户通过支付少量代币完成模型训练目的。

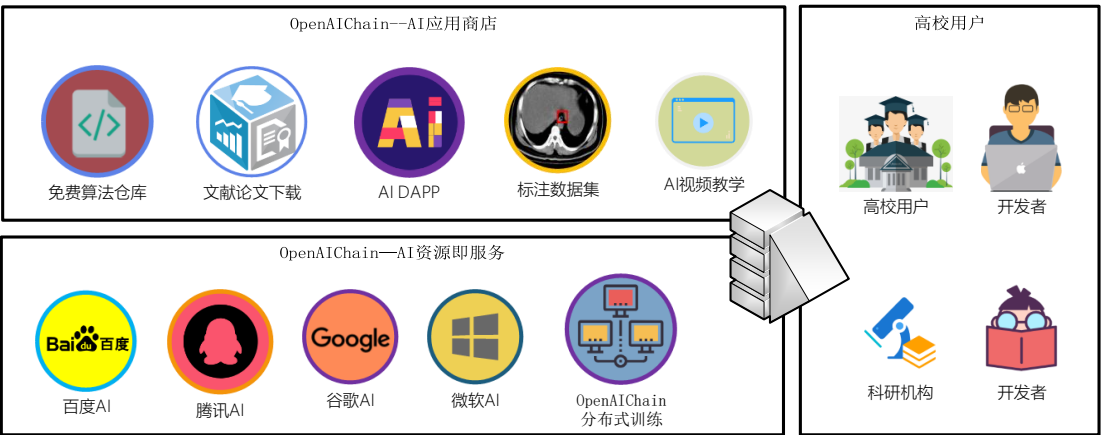


图 21.面向开发者--资源整合平台

5. 代币销售众售规则

5.1 OpenAI Coin（OAC）代币发行

OpenAIChain 的官方代币是 OAC，代币数量恒定永远都不会有增发，OpenAIChain 链代币总额大约为 30 亿枚。官方为了激励开发者提交更加丰富和优秀的模型、激励数据提交者提交更加丰富数据量，将会设置 55%比例代币进入市场，其中 20%分配给早期投资者。

5.2 代币分配方案

OpenAIChain 的代币分配方案如下：

团队	10%	团队内部分配
基石及私募	20%	基石投资人及机构投资者，其中私人预售10%
基金会，OpenAILab	15%	管理基金会，支持发展，负责实现OpenAIChain迭代开发
社区奖励	5%算法竞赛	定期组织算法竞赛，鼓励全球开发者参与AI项目研发
	15%分中心节点	奖励分中心节点
	5%顾问、学术	OpenAIChain学术、商业、投资顾问
任务奖励	30%	用于奖励数据标注者、任务完成者、算力、算法贡献者
品牌推广	10%	用于登录各个交易所，接入全球各大平台，品牌推广等

表 1.代币分配细节

OpenAIChain 官方代币分配如表 1 所示。

5.3 代币销售规则说明

代币在不同众售期有不同的优惠比例，以正式启动代币销售时公示的版本为准。

6. 应用和未来工作

6.1 应用案例

6.1.1 数据交互服务

OpenAIChain 将收集数据公布于链上，部分数据给予出售，但大部分数据供公司、训练者使用，下面分为两种情况：

- 出售数据：面向特定公司出售链上数据，数据价值由数据珍惜程度规定；
- 公有数据：公有数据供所有公司调用，这部分数据为加密数据，无法下载到本地，调用公有数据仅收取使用数据少量的代币费用以做良性数据采集循环，且一次支付无限次使用，让公司、个人都拥有这部分数据。

6.1.2 信息社交服务

· 知识共享与知识变现服务：打造社交问答 APP，根据用户发文、发出算法数量，以及文章算法点赞数给予用户代币奖励，作为知识盈利，致力于汇总全网模型训练知识。文章阅读者可以对文章点赞评论以作为文章好坏区分。

· 信息推送服务：根据用户的交易信息、用户画像，给与用户推送每日 AI 新闻、模型分享动态。

· 学术汇总服务：收集全网各种开源数据集，供开发者、科研工作者训练，推送各种学术会议信息，学术会议文献集汇总。

6.1.3 跨学科交叉服务

- 跨学科交流合作：计算机专业与生物、医学领域等来完成学科交叉探索；
- 跨学科数据标注采集：对数据进行标注（如医学领域学生可对医疗影像进行标注）、提供不同学科数据信息，增大学科交流信息；

OpenAIChain 链致力打造共享人工智能平台

6.1.4 人工智能应用

- 自动问答：聊天机器人，根据用户对话生成回答；
- 行业知识图谱：专家系统，可以应用在医疗、咨询等行业；
- 自动驾驶模型：生成自动驾驶模拟环境，学习者参与自动驾驶学习；
- 语音合成：根据用户的语音数据生成另一段风格相似的语音；
- 人脸属性预测：根据用户上传的人脸数据对年龄、性别、情感等属性作出判断；

6.1.5 竞技比赛

OpenAIChain 将定期与各大人工智能企业举办 AI 竞技比赛，汇集全球优秀 AI 开发者想法并公开训练算法，促进 AI 行业算法发展。同时，将比赛优秀获奖者推荐给各大企业。

6.2 未来工作

OpenAIChain 未来工作就是将主链上线，逐步实现上述想法。

7. OpenAIChain 发展规划

7.1 开发路线图



7.2 未来迭代规划

随着 DAG、Hashgraph 的发展，OpenAIChain 将会对底层版本进行迭代更新，融合最新的区块链架构技术，对底层公链进行升级迭代。

7.2.1 底层架构迭代

当 OpenAIChain 代码本身出现漏洞，通常采取系统升级。出现漏洞需要经过代码委员会进行分析、测试和审核，提交至决策委员会报备。当出现以下重大漏洞（不限于）采取系统升级：

- 影响用户资金
- 重大安全问题
- 影响系统安全

当出现较小的漏洞时，直接由代码委员会进行补丁。

7.2.2 商业应用迭代

OpenAIChain 将会是部分开源的项目，OpenAIChain 希望通过技术上的创新、理念上的创新将区块链与现实链接起来。OpenAIChain 基金会会选择合适的第三方合作，进行行业和应用迭代。

8. OpenAIChain 治理架构

8.1 基金会设立

OpenAIChain 基金会（以下简称“基金会”）是在非营利性实体。OpenAIChain 基金会将作为 OpenAIChain 项目的倡导实体，致力于 OpenAIChain 项目的开发建设和治理透明度倡导及推进工作，促进开源生态社区的安全、和谐发展。OpenAIChain 项目团队委托具有公信力的第三方机构，协助团队设立基金会实体，并代为维护实体架构的日常运营与报告事务。而基金会设立后，即遴选适当的社区参与成员，加入基金会职能委员会，共同参与实际的管

理与决策。

8.2 基金会治理原则

OpenAIChain 基金会治理结构的设计目标主要考虑项目开发的可持续性、战略制定的有效性、管理有效性、风险管控及项目的高效运营。基金会在治理结构方面提出以下原则：

(1) 中心化治理与分布式架构的融合：完全的去中心化带来的可能是绝对的“公平”也可能是更多的“低效”。因此 OpenAIChain 基金会仍会在管理架构上吸纳一定的中心化治理的核心思想，包括战略决策委员会的最高决策权限以及重大事项的集中议事权力等，以提高整个社区运营的效率。

(2) 职能委员会与职能单元共存：基金会在日常事务下，将设立常驻的职能单元，例如研发部门、市场开发部门、运营部门、财务及人力资源部门等，以处理经常项事务。同时，设置专业的职能委员会，对基金会的重要职能事项进行决策。与职能单元不同，职能委员会以虚拟架构存在，委员会的成员可以来自全球，也无需全职办公。但其必须符合委员会专家资质的要求，并能够承诺在委员会需要进行议事的时候出席并发表意见。职能委员会也会设置定期会议制度，以保证重大决策事项的有效推进。

(3) 风险导向的治理原则：风险管理原则为先保证了基金会做出重要决策时，充分考虑了风险因素、风险事项以及其发生的可能性和影响，并通过决策制定相应的应对策略。从而保证 OpenAIChain 项目的发展与迭代走在一个正确的道路上。

(4) 技术与商业并存：OpenAIChain 项目秉持技术与商业的紧密结合为宗旨，以促进区块链技术在人工智能市场的落地。OpenAIChain 基金会的设置，同样也遵循这一宗旨。即便基金会以非盈利机构的形式存在，但基金会希望尽最大程度获得商业世界的认可，赢取商业应用的收益，同时反馈到基金会以及社区，用以进一步推进基金会以及 OpenAIChain 项目的开发与升级。

8.3 基金会组织架构

基金会治理结构的设计目标主要考虑开源社区项目的可持续性、管理有效性及数字资产的安全性。基金会由团队人员和职能委员会组成，组织架构主要由决策委员会、代码审核委员会、财务及人事管理委员会和市场及公共关系委员会组成。基金会成立初期，决策委员会由基金会主席、团队核心人员和早期支持者成员组成，每期任期为二年。

8.4 基金会人力资源管理

OpenAIChain 为确保技术层面的开发顺利和基金会运营持续有效，基金会将致力于招聘优秀的技术开发人员以及人工智能领域的专业人才。

8.5 基金会风险评估及决策机制

区块链作为一项创新技术，不仅仅是在计算机核心技术上有颠覆性的突破，同时也是对人工智能领域的革新。因而风险管理体系的重要性不言而喻。OpenAIChain 基金会秉持建立以风险为导向的可持续经营的区块链社区。OpenAIChain 基金会将对基金会的运作进行持续性的风险管理。包括风险体系设立、风险评估、风险应对等一系列活动。对于重大风险，均需基金会战略决策委员会商议讨论并决策。基金会将根据事件特性，例如事件影响程度、影响范围、影响代币量和发生的概率进行分级，按照优先级进行决策，对于优先级高的事件，尽快组织基金会相关委员会进行决策。

9. OpenAIChain 核心团队成员

· **尹成** 毕业于清华大学，微软人工智能领域全球最具价值专家，微软 Tech.Ed 大会金牌讲师。资深软件架构师，Intel 软件技术专家，著名技术专家，具备多年的世界顶尖 IT 公司微软谷歌的工作经验。具备多年的软件编程经验与讲师授课经历，并在人机交互，教育，信息安全，广告，区块链系统开发诸多产品，具备深厚的项目管理经验以及研发经验，拥有两项人工智能发明专利，与开发电子货币部署到微软 Windows Azure 的实战经验。

· **吕金蕾** 5 年区块链研究经验，专注于区块链+安全领域。主导过多个区块链安全方案，北美区块链协会高级研究员，2012 年开始关注和研究区块链技术，在业内核心媒体发表多篇专栏文章。

· **孙若禹** Qbao 联合创始人&COO，10 年信息技术和互联网经验，区块链专家。曾就职于 Capgemini，Alcatel，YUM 等企业。同时也是 ETHCHINESE 和 BLOCKCHAIN CLASSROOM 的联合创始人。

· **谭祎** 百度资深区块链工程师，专注于数字货币交易所研发和 NEM 区块链研发与应用，APEC 未来学院顾问委员会委员、丝绸之路创新设计联盟专家组成员。在多家研究机构

OpenAIChain 链致力打造共享人工智能平台

就职并从事区块链交易所系统架构的研究工作。

· **董德俊** 北京理工大学计算机科学硕士。360 资深工程师，中国软件行业协会区块链创业学院及专委会专家，具备多年的 C/C++，go 编程经验。专注于数字货币交易所研发和 NEM 区块链研发与应用。密码学专家，10 年以上软件开发经验。

· **毕远** 英特尔资深区块链工程师，电子合同，智能知识产权区块链项目研发负责人，研究方向包括运营与金融、供应链、区块链，经济网络和机器学习应用，并在 INFORMS、IEEE、IIE 等会议及期刊上发表 10 余篇文章。全球首家区块链上市公司 DigitalX 和澳洲最大区块链资产交易平台 ACX.io 技术顾问。

· **李华** 深圳大学硕士学位，技术总监，架构师。11 年分布式系统架构经验，专注于数据后台处理以及分布式相应系统，2017 年研究区块链至今。

· **郭一祺** 华南师范大学软件工程硕士在读，主要研究方向区块链及自然语言处理。

· **欧政** 运营总监，曾任职国际互联网金融平台首席运营官，致力互联网运营的创新与推广，品牌建设与传播。10 年股票二级市场实战交易经验，2015 年致力研究数字货币交易市场。

10. OpenAIChain 顾问

10.1 技术顾问

· **李滨** 上海微能投资管理有限公司董事长，英特尔创新加速器战略顾问和特聘导师。他创立的微能创投加速器，专注于机器人、人工智能、物联网和大数据等新兴技术领域，依托开放创新生态，为高科技创业者建立创投资本和加速器网络。为英特尔定制的 A.C.T 创投加速营已经成功加速了上百个高科技创业项目，部分优秀团队成功获得英特尔投资联盟机构的投资。曾在美国 IBM 公司、苹果公司、麦克菲公司担任总经理等高级管理职务，在信息技术软件、硬件和咨询服务业务方面有 20 多年的管理经验，在高科技产品市场、分销、品牌管理和战略管理方面有自己独到理解和资源体系。中欧国际工商学院中国创新中心顾问，中欧国际工商学院创业实验室导师，上海纽约大学创业加速器导师。

· **邱浩** 清华大学学士学位。在 TMT 领域拥有 19 年行业从业经验。创立联基金之前，从 2011 年到 2014 年，邱浩作为创新工场合伙人，参与主投了墨迹天气，乐视 TV，快牙，

OpenAIChain 链致力打造共享人工智能平台

51VV, 蜻蜓 FM, 易邀中国, 极路由, Blink 等 20 多个项目, 其中超过 8 个项目估值过亿美金。并参与大量投后管理工作, 包括友盟, 要出发, 知乎, 安全宝等。加入创新工场之前, 从 2007 年初到 2011 年底, 邱浩是晨兴创投北京公司负责人, 主投和参与投资的项目包括 YY, UC 浏览器, 到家美食会, 尚品网, 龙焱科技等。从 2004 年到 2006 年, 邱浩在麦肯锡担任高级管理咨询顾问。邱浩在 2000 年和 2006 年分别两次创业。邱浩还在中国惠普的企业系统部门工作了 5 年, 曾担任中国惠普金融行业解决方案销售总经理。邱浩目前还担任清华大学校友总会投资协会理事以及清华大学校友总会 TMT 协会理事。

10.2 学术顾问

罗平教授 清华大学

10.3 商业顾问

· **刘春河** 北京邮电大学硕士, 赤子城创始人、CEO。赤子城于 2014 年 6 月获得梅花天使和明势资本 200 万美金的天使投资, 2014 年底获得安芙兰国泰数千万人民币的 A 轮融资, 2015 年年初获得海通开元 2 亿元 B 轮融资, 2015 年 8 月完成数亿元 C 轮融资, 2016 年 4 月获得数亿元 D 轮融资。

· **陶锋** 清华 x-lab 首席培育教练、行动学习实验室创办人。清华 MBA 校友, 有超过 10 年的互联网行业经验以及 5 年多的企业管理咨询行业经验。曾参与创办国内最早的汽车行业垂直网站 (veryauto.com) 和国内最早的商务社交网站 (tianji.com), 以及国内第一家 3D 虚拟世界游戏 (hipihi.com), 拥有丰富的互联网商业模式创新、产品策划、研发、运营管理以及营销推广等多方面的经验。并且, 作为创业核心团队成员, 在创业过程中也积累的宝贵的创业经验。此后, 在和君集团工作期间, 为超过 20 多家企业提供咨询服务, 主要方向为传统行业的互联网转型。

· **Mike Vella** 加利福尼亚大学, 伯克利分校法律博士, 拥有二十多年的执业经验, 协助客户管理其国际经营活动中发生的各种风险。他协助全球性公司解决其在亚洲各地的商业纠纷、合规问题和知识产权诉讼等事项。Mike 还代理中国公司经办其海外诉讼案和国际仲裁案, 代理公司有高通 (Qualcomm)、Applied Materials、Chinmax Medical Systems 等。2016 年于知识产权管理杂志 (Managing IP) 获“专利明星律师”称号。

10.4 合作机构

11. 投资机构

12. 免责声明与风险提示

除本白皮书所明确载明的之外,OpenAIChain 基金会不对 OpenAIChain 或项目代币 OAC 作任何陈述或保证(尤其是对其适销性和特定功能)。任何人参与 OpenAIChain 的售卖计划及购买 OAC 的行为均基于其自己本身对 OpenAIChain 和 OAC 的知识和本白皮书的信息。在无损于前述内容的普适性的前提下,所有参与者将在 OpenAIChain 项目启动之后按现状接受 OpenAIChain, 无论其技术规格、参数、性能或功能等。

OpenAIChain 基金会在此明确不予承认和拒绝承担下述责任:

- (1) 任何人在购买 OAC 时违反了任何国家的反洗钱、反恐怖主义融资或其他监管要求;
- (2) 任何人在购买 OAC 时违反了本白皮书规定的任何陈述、保证、义务、承诺或其他要求, 以及由此导致的无法付款或无法提取 OAC;
- (3) 由于任何原因 OAC 的售卖计划被放弃;
- (4) OpenAIChain 的开发失败或被放弃, 以及因此导致的无法交付 OAC;
- (5) OpenAIChain 开发的推迟或延期, 以及因此导致的无法达成事先披露的日程;
- (6) OpenAIChain 源代码的错误、瑕疵、缺陷或其他问题;
- (7) 未能及时且完整的披露关于 OpenAIChain 开发的信息;

OpenAIChain 基金会相信, 在 OpenAIChain 的开发、维护和运营过程中存在着无数风险, 这其中很多都超出了 OpenAIChain 基金会的控制。除本白皮书所述的其他内容外, 每个 OAC 购买者还均应细读、理解并仔细考虑下述风险, 之后才决定是否参与 OAC 的售卖计划。

【参考文献及引用】

- [1] Satoshi Nakamoto. Bitcoin: A peer-to-peer electronic cash system. <https://bitcoin.org/bitcoin.pdf>, 2009.
- [2] Ethereum white paper. <https://github.com/ethereum/wiki/wiki/White-Paper>.
- [3] Steem. 一个激励人心的、基于区块链的社交媒体平台.steemwhitepaper-cn-v2.pdf
- [4] Gentry C, Halevi S, Smart N P. Homomorphic Evaluation of the AES Circuit[M]// Advances in Cryptology - CRYPTO 2012. Springer Berlin Heidelberg, 2012:850-867
- [5] Ramachandran A, Kantarcioglu M. SmartProvenance: A Distributed, Blockchain Based DataProvenance System[C]// the Eighth ACM Conference. ACM, 2018:35-42.
- [6] King S, Nadal S. PPCoin: Peer-to-Peer Crypto-Currency with Proof-of-Stake. 2012.
- [7] Yuan Yong, Wang Feiyue. Blockchain: the state of the art and future trends[J]. Acta Automatica Sinica, 2016, 42(4): 481-494
- [8] Eyal I, Gencer A E, Sirer E G, et al. Bitcoin-NG: a scalable blockchain protocol[C]//Proceedings of the 13th USENIX Symposium on Networked Systems Design and Implementation, Santa Clara, Mar 16-18, 2016. Berkeley: USENIX Association, 2016: 45-59.
- [9] Le Q V. Building high-level features using large scale unsupervised learning[C]// IEEE International Conference on Acoustics, Speech and Signal Processing. IEEE, 2013:8595-8598.
- [10] Rivest R L, Adleman L, Dertouzos M L. On data banks and privacy homomorphisms[J]. Foundations of Secure Computation, 1978:169-179.
- [11] Josep Domingo i Ferrer. A new privacy homomorphism and applications[J]. Information Processing Letters, 1996, 60(5):277-282.
- [12] Howard J H. Scale and performance in a distributed file system[J]. ACM SIGOPS Operating Systems Review, 1987, 21(5):1-2.
- [13] Borthakur, Dhruba. "HDFS architecture guide." Hadoop Apache Project 53 (2008).
- [14] Zheng, Ling, Yanxiang Hu, and Chaoran Yang. "Design and research on private cloud computing architecture to support smart grid." Intelligent Human-Machine Systems and Cybernetics (IHMSC), 2011 International Conference on. Vol. 2. IEEE, 2011.
- [15] Benet J. IPFS - Content Addressed, Versioned, P2P File System[J]. Eprint Arxiv, 2014.
- [16] Veena P, Ahluwalia G, Panikkar S. An Economy of Things—A Visionary Architecture and Monetization of Devices with Blockchain. IBM Inter Connect, 2016.
- [17] Mashey B J R. Big Data and the Next Wave of InfraStress[J].
- [18] James Manyika, Michael Chui, Brad Brown, et al. Big data: The next frontier for innovation, competition, and productivity[J]. Analytics, 2011.
- [19] Wikiprdia. Big data[EB/OL].2009. [2016-11-11]. https://en.wikipedia.org/wiki/Big_data.
- [20] Xiaojin,Zhu. Semi-Supervised Learning Literature Sur-vey[J]. 2005, 37(1):63-77.

- [21] Hinton G E, Osindero S, Teh Y W. A Fast Learning Algorithm for Deep Belief Nets[J]. Neural Computation, 2006, 18(7):1527-1554.
- [22] Schölkopf, B, Platt, J, Hofmann, T. Greedy Layer-Wise Training of Deep Networks[J]. Advances in Neural Information Processing Systems, 2007, 19:153-160.
- [23] Llm. <https://llvm.org/>. Accessed: 2017-08-01
- [24] Page L. The PageRank Citation Ranking : Bringing Order to the Web[J]. Stanford Digital Libraries Working Paper, 1998, 9(1):1-14.
- [25] Zhang, W., Gupta, S., Lian, X., & Liu, J. (2015). Staleness-aware async-sgd for distributed deep learning. arXiv preprint arXiv:1511.05950.
- [26] The Stage 1 Casper Contract. <https://github.com/ethereum/casper/>. Accessed: 2017- 08-01.