NEBULA AI 智云链（NBAI）去中心化人工智能区块链白皮书

Nebula AI Team

2018 年 4 月

V 2.7

摘　要

区块链技术为人类提供的数字化信任机制，提升了价值传递的效率且降低了成本，真正可信且高效的价值互联网世界正迎面走来。同时，区块链应用创新欣欣向荣，昭示着公共服务发展和产业创新革命的新方向。近年来，人工智能领域取得了许多重大突破，并在全球范围内掀起了狂热的研究与应用浪潮。人工智能现已渗透到人类社会的每个缝隙，并将成为推动人类社会变革的重要基石。

Nebula AI 致力于构建去中心化的人工智能计算基础链（智云链），通过将 GPU 矿机转化成人工智能计算服务来减少传统工作量证明的能源耗费。在 Nebula AI 区块链上，研发人员可以基于 Nebula AI 的通用编程接口设计自己的人工智能 App，通过发布免费或者付费 App，或通过用户付费使用获得 NBAI 代币收入。记录在智云链上的人工智能交易将不可逆转，分布式的计算网络也保证了高并发、低延迟的计算能力，GPU 矿机的转换使得提供更加经济高效的人工智能服务成为可能。

Nebula AI 将与大规模的第三方互联网数据中心合作，为 AI 计算提供充足的算力。Nebula AI 也已经在加拿大建立了人工智能人才培养中心，并致力于传播人工智能行业最新应用和知识，向社会输送优秀人才。系统搭载的量化金融，图形识别等相关链上应用也在同步发展中。

完善的智云链生态系统集合了 DAI App、科研应用、高校教育等顶层应用和智云链区块链、人工智能矿机以及人工智能数据中心的底层支持。创新的智云链生态系统的经济模型则实现了一套完整的价值流转经济增值系统。

声　明

本文作为一份技术白皮书，介绍了 Nebula AI 的智云链平台和智云链生态系统的当前与未来发展情况。本文仅供参考，不可作为未来意图的声明。除非另有明确规定，本文中拟议的产品和创新目前正在开发中。对该种技术和创新的成功开发或实现本文中所述的任何其他活动，Nebula AI 概不做出任何保正或声明，且在法律允许的范围内，概不承担法律或其他方式暗示的任何保正。任何人员不得依赖本文件的内容或从中得出的任何推论做出决策，包括与 Nebula AI 的任何互动或本文提及的技术。对于个人由于依赖与 Nebula AI 相关的任何信息或意见，本白皮书中所含的智云链平台和智云链生态系统的相关信息或意见或与任何进一步咨询相关的信息面招致的任何损失或损害（无论是否可预见），Nebula AI 概不承担任何责任，尽管出现任何疏忽或不慎。

本白皮书中包含的信息来自于 Nebula AI 认为从可信任来源所获得的信息，并如实反映信息，但 Nebula AI 概不担保或保证上述信息的准确性、完整性或适用性。您或您的任何雇员、债权人、证券持有人或其他权益持有人或任何其他人不得依赖该信息，不得依赖该信息赋予的权利或补救。本白皮书所表达的任何意见均反映本文作者目前的判断，且不一定代表 Nebula AI 的意见。本文反映的意见可能变更，恕不另行通知。若本文所述的任何事项或任何意见、投资、预测或估计发生变化或随后有误，Nebula AI 概无义务修改、修正或更新本文件或以其他方式通知读者。

对于本白皮书内容或遗漏招致的任何明示或暗示声明、意见或信息而对任何个人导致的损失，Nebula AI 与其雇员概不承担任何责任或义务。Nebula AI 及其顾问均未独立核实任何信息，包括本文中包含的预报、前景和预测。尽管我们竭力确保本文所述事实陈述准确无误，但本文所载的所有估计、预测、预报、前景、意见表达和其他主观判断均基于本文件截至当日被认为合理的假设，且不得被解释为所述事项即将发生的声明。本文提及的任何计划、预测或预报均可能由于多种风险因素而无法实现，包括但不限于技术发展、法律或监管风险、市场波动、部门变动、企业行为或无法获得完整、准确的信息。每位读者自行依赖其知识、调查、判断和评估，以确认信息准确性和完整性。

本文仅可在 www.nebula-ai.com 访问，未经 Nebula AI 事先书面同意，任何个人不得以任何目的重新分发、复制或转让给任何其他个人或部分或全部出版本文的内容。通过访问本白皮书，本白皮书的读者同意受上述限制的约束。

目录

1 技术与行业纵览

1.1 价值互联网现状

传统的互联网是基于历史内容的，并不创造新的价值，业界称之为信息互联网。而区块链技术能够通过建立高效可信赖的价值传输系统，从而将互联网进化为构建社会信任体系的网络基础设施，使互联网能够产生新的价值，实现价值的有效传递，业界将此称为价值互联网。

1.1.1 区块链的发展

区块链技术是建立于分布式系统、计算机网络、密码学和数据结构等多领域研究成果基础之上的综合性技术系统。区块链由多方共同记录行为与维护数据，通过应用密码学确保数据的传输和访问安全，数据使用链式结构存储，只能被读取或写入，从而能够保证其一致性、防止篡改且不可抵赖。以比特币和以太坊为代表的区块链技术，通过加入数据加密、共识机制、时间戳和经济激励等技术与手段，在分布式节点之间实现去中心化的点对点信用交易，从而解决了传统中心化机构中普遍存在的交易周期繁琐低效、高成本和数据存储不安全等问题，从而成为了现代数字加密货币体系的核心技术。这种技术系统可以实现所有参与者的信息共识、共享、共责，能够被完美移植到绝大多数基于信任的商业模式和组织架构的底层应用中。

中本聪（Satoshi Nakamoto）于 2008 年发表比特币设计论文《比特币：一种点对点的电子现金系统》，作者希望可以创建一套新型的去中心化电子支付系统，这套系统 “基于密码学原理而不是基于信用，使得任何达成一致的双方能够直接进行支付，从而不需要第三方中介参与” [13]。由此以比特币为代表的区块链技术开始为世人所知。

业界和学术界通常将区块链技术划分为两代：

- 1.0 比特币 — 解决了加密账本和去中心化支付的问题。
- 2.0 以太坊 — 丰富了区块链技术的应用价值。以太坊使用的智能合约可以使用虚拟机和合约编程，给数字货币的发展提供了新的思路。同时大量的 DApp 和 ICO 金融创新油然而生，为金融市场开辟了新的疆土。

比特币作为区块链最初的应用，实现了去中心化电子货币记账系统的模式。比特币根据特定算法依靠完成计算任务产生，不依赖于任何个人或机构，从而保证了

比特币网络分布式记账系统的一致性。维塔利克 · 布特林（Vitalik Buterin）在其设计的以太坊（Ethereum）中应用了智能合约的概念 [4]，为我们提供了具有图灵完备性的区块链通用框架。

应用区块链技术能够在网络中建立可信的点对点传输，这为我们提供了新型的社会信任机制，既支持共同决策又能保护个体权益，既公开交易信息又保护节点隐私，这种机制提高了价值传递的效率且降低了成本，为数字化经济的发展奠定了新基石，标志着人类社会开始从信息互联网向上进化，构建真正可信且高效的价值互联网世界。同时，区块链应用创新欣欣向荣，昭示着公共服务发展和产业创新革命的新方向。

1.1.2 DApp 与人工智能

DApp（Decentralized Application） 是一种代码运行在去中心化 P2P 网络服务器节点的应用程序，它主要由前端表现层，后台服务器和智能合约这三部分组成。随着以太坊的快速发展，数十万 DApp 已于各行各业应运而生，价值互联网生态系统日渐丰满。

近年来人工智能领域取得了许多重大突破，并在全球范围内掀起了对其狂热的研究浪潮。人工智能的研究和应用现已渗透到人类社会的每个缝隙，DApp 中也不乏人工智能的身影。然而人工智能的研究需要很强的计算能力，早已从初期的 CPU 运算全面提升至 GPU 计算，大规模应用部署则对硬件性能和系统并发处理有更高的要求。

Nebula AI 区块链作为新一代的人工智能区块链，致力于解决人类走向人工智能过程遇到的计算能力需求，加快资源的跨地区流转以及更便捷的编写集成去中心化的人工智能应用，从而将区块链的微支付，超级账本，去中心化特性和人工智能应用完美集成在一起，实现从 DApp + AI 到 DAI App 的目标。

Nebula AI 是一个去中心化的人工智能计算基础链。通过将 GPU 矿机转化成人工智能计算服务来减少传统工作量证明的能源耗费。在 Nebula AI 区块链上，研发人员可以基于 Nebula AI 的通用编程接口设计自己的人工智能 App，通过发布免费或者付费 App 的方式，通过用户的使用获得 NBAI 代币收入。普通用户的付费一部分用于人工智能应用的使用，一部分则由人工智能 App 间接支付给 Nebula AI 区块链。记录在 NBAI 上的人工智能交易将不可逆转，分布式的计算网络也保

证了充分的计算能力，GPU 矿机的转换让提供更加低廉的人工智能服务成为可能。Nebula AI 已经在加拿大建立了人工智能人才培养中心来加速人工智能、区块链相应人才的培养，并且计划与大规模的第三方互联网数据中心合作，为 AI 计算提供算力。系统搭载的量化金融，图形识别等相关链上应用在同步发展中。

Nebula AI 智云链将为价值互联网注入新鲜的血液，为全球人工智能开发提供经济高效的基础服务。

1.2 市场前景

区块链技术已实现全球化应用部署，各国都在密切关注区块链的发展，谋划区块链开发应用的发展道路。根据市场研究机构 Gartner 预测，基于区块链的业务将于 2020 年达到 1000 亿美元，除了在金融界的大规模应用之外，区块链还会在制造业和供应链行业创造超过一万亿美元的价值。克劳斯 · 施瓦布（Klaus Schwab）认为，区块链是继机械化、电气化和数字化之后的第四次工业革命，预计到 2025 年之前，全球 GDP 总量的 10% 将利用区块链技术进行数据储存 [18]。Marketsand Markets 预测，用于提高企业运作效率的全球区块链应用和方案供应商的年均增长值将于 2016 年至 2021 年间达到顶峰 [9]。区块链技术的市场前景主要在于社会公共服务和经济模式优化两方面：

在社会公共服务层，区块链技术正在渗透到社会保障、知识产权、公共管理等各个方面，并主要围绕四个领域发展：身份验证、鉴证确权、信息共享以及透明政府。英国政府在 2016 年发布报告《区块链：分布式账本技术》，第一次从国家层面探讨了分布式账本在政府事务中的重要应用 [21]。随后，美国成立了 “国会区块链小组”，俄罗斯、新加坡、迪拜、日本、中国等政府都纷纷加速推进区块链技术的社会应用 [15]。在区块链技术的分布式共识、透明开源和社会协作的底层哲学的影响下，公共服务领域实现了从数据管理流程的优化到治理思维的全面改变，有助于提升公众参与度，降低社会运营成本，提高社会管理的质量和效率，对社会管理和治理水平的提升具有重要的促进作用。

在经济模式优化层，区块链经济的核心设计思想在于商业逻辑的重构，打造未来金融和经济的新格局，而非仅仅一场技术革命 [6]。早在 2015 年，区块链就已经成为美国创投中获得融资最高的板块。当前全球区块链项目已经超过 2000 个，全球加密数字资产总体价值达到 900 亿美元。区块链在金融、共享经济、物联网等方

面存在很高的应用价值，已经吸引了高盛、花旗、纳斯达克、德勤、爱彼迎等商业集团的积极布局。区块链/数字资产领域的用户人群也正在快速增加，从 2013 年初的全球 200 万用户，增长到 2017 年初的 2000 万用户 [19]。在区块链体系中，参与者可以不需要了解对方基本信息的情况进行交易，实现了“无需信任的信任”，改变了传统模式中以第三方为中心的信任模式，经济体系可以脱离当前通过制度约束或第三方机构背书，双方直接实现价值交付。这种基于区块链经济的解决方案，可以改善现有的商业规则，构建新型的产业协作模式，提高协作流通的效率。区块链可为经济社会转型升级提供系统化的支撑 [17]。其显著优势在于优化业务流程、降低运营成本、提升协同效率，这个优势已经在金融服务、供应链管理、智能制造以及教育就业等社会各领域显现出来。

人工智能产业在经历了 60 年的起伏之后，终于伴随着机器学习的崛起而重新复苏，如今已经在全球范围形成新一轮的抢位发展态势，各国纷纷吹响探索人类智慧奥秘的号角。全球人工智能市场的规模在 2015 年达到 1683.9 亿，2016 年随着全球各领域对人工智能研发的加强和重视程度的提升，行业市场规模提升超过 1900 亿 [12]。根据市场发展需求，前瞻估算至 2018 年，全球人工智能市场规模有望达到 2700 亿。

DApp 在未来将构成了价值互联网的骨干，人工智能将涉及所有应用领域，区块链作为前两者的基础设施必将大行其道，势必带来对传统互联网、人类社会以及自然生态环境的重大变革。

1.3 现存问题

1. 高度中心化

谷歌亚马逊均开始提供人工智能计算云服务。但是他们都是单一商业化的公司，他们会基于自身的利益和政府组织等的压力，如遇到特殊情况将会随时切断服务，用户将丧失其服务。例如谷歌在中国被中国政府所禁止运营导致中国用户无法使用其相应的服务。

区块链是一种新型去中心化协议，它通过分布式账本（一类分布在多地址、多地区或多参与者的数据库）这个载体，安全地存储数据信息 [3]。区块链基于 “去中心化” 的架构，任意节点间的权利和义务是均等的；系统中的数据块由所有节点共同维护，每个节点分享权利和义务；通过分布在全球的节点进行验证，确保信息不

可伪造和篡改；从技术上保证交易的进行，无需第三方结构提供信任机制。企业利用去中心化的分布式账本技术处理、验证交易或者其他类型的数据交换，记录存储在账本中，一旦大多数参与者达成共识，其中每个记录都将获得时间戳及独有的加密签名。分布式账本的所有参与者可以浏览多有存疑的记录，提供了可验证及可审计的信息历史 [11]。这种技术保证了只要还有一个节点在运营，就不可能关闭整个网络。从而使得设计一个无法被封禁的去中心化 AI 云服务成为了可能。

2. 数据隐私安全

尽管中心化的公司有各种安全保障协议，但是当遭遇内部职员泄密事件时，公司很难保证数据隐私的安全。另外，在被政府要求交出数据时，中心化公司受限于所在国的地域限制，只能选择跟政府合作并交出数据，因此用户的数据安全并不能得到 100% 的保证。

区块链基于密码学技术通过特定算法，依靠一定的共识机制，点对点交易，信息存储在各节点，无需信任单个中心，是一种基于加密技术的低成本、高安全、可定制和封装的去中心化信任解决工具 [22]。每个节点通过保存一套完整历史数据库的副本，参与维护信息的安全性和准确性。区块链的点到点加密技术可以很好的保证除了私钥的持有者，其他用户即使拿到了数据也无法解密使用。这对于各种高价值的训练数据和训练模型具有非常大的意义。区块链在数据安全方面体现的优势有:

- 利用高冗余的数据库保障信息的完整性。
- 利用密码学的相关原理进行数据验证，保证数据的不可篡改。
- 运用多私钥进行访问权限控制。

3. 维护成本

中心化的计算中心因为需要专人维护，所以需要消耗大量的人力成本。而使用区块链的微支付功能，可以使得支付维护费用的过程变得非常简单，每个人都可以出借自己的计算能力。共享经济的模式极大减少了维护的人力开销，从而降低了计算成本。

4. 哈希计算效能

目前以太坊，Zcash 等 GPU 工作量证明耗费了大量的电力与哈希运算上，这些 GPU 的计算能力本可以用于 AI 计算，而不是单纯的用作工作量证明。一项最

新研究显示，比特币挖矿今年消耗的电量已经超过 159 个国家的年均耗电量。如此高的耗电量称为一个亟待解决的问题。Digiconomist 估计比特币挖矿每年消耗约 30.14 TWh 电量。远高于爱尔兰 25 TWh 的年均耗电量 [8]。事实上，荷兰银行 ING 最近的论文显示，一次比特币交易消耗的电量足够一个家庭一整月的用电量。Digiconomist 还发现，当今热度第二的加密货币以太坊消耗的电量也超过很多国家的耗电量 [1]。

5. 区块链应用生态环境的建立

随着区块链上各种应用（DApp）的快速增长，良好的生态环境是提高用户体验的根本所在。这涉及用户如何在海量的区块链应用中检索自己期望的 DApp，如何激励开发人员为用户提供更多的 DApp，以及如何帮助开发人员更快的构建更好的 DApp。以以太坊为例，基于以太坊的 DApp 总数已经数十万个，试想如果区块链世界中的 DApp 接近苹果 App Store 里应用总量规模的话，如何发现并找到用户期望的 DApp 就是个很大问题。随着区块链技术的普及，越来越多区块链技术之上的应用场景被挖掘出来。区块链技术的应用场景已经从最初的数字化货币本身逐步扩展到更多的场景及用户群体中。例如，以以太坊为代表的社区在区块链技术中引入智能合约的概念，Ripple 则使用区块链技术实现了全球的结算系统。随着应用场景的多样化，用户对区块链技术的诉求也日益增加，我们已经看到很多挑战。

1.4 项目目标

为了改善目前中心化云计算的现状，我们利用区块链技术的去中心化特性将人工智能机器在全球范围内进行计算能力的租用和分配。区块链加密技术有效规避了内部泄密问题的存在，而分布式的 AI 计算单元的维护则交给了大大小小的人工智能计算单元的拥有者，极大地减少了维护的工作量。这个总目标，可以拆分成以下几个子目标:

1. 共享 AI 计算平台

共享 AI 计算设备平台将解决 AI 设备的拥有者和使用者之间的不平衡的需求状况。AI 计算设备的拥有者无法 100% 得发挥其计算潜力从而导致了部分计算资源的闲置。与此同时，大量需要人工智能的计算能力的用户又无法得到经济高效的 AI 计算资源。通过区块链技术完成的点到点支付以及区块链记账技术可以让共享

AI 算力以最便捷的方式完成支付和共享。

2. AI 物理计算单元

大量的 GPU 计算矿机可以转换成 AI 计算单元，从而从单纯的哈希计算转换成更有意义的 AI 任务计算。由于 AI 计算的特殊性，需要预装指定的系统并且定期更新客户端，包括记账系统，才能更好的发挥硬件的性能以及分享 AI 计算能力。

3. 去中心化 AI 应用

去中心化 AI 应用（Decentralized AI Application）接入系统时需要对应的接口让 DAI App 程序员以便捷的方式进行开发调用以使用平台中强大的计算能力。主要包含支付 API，计算能力估算 API，工作量预估 API 等等，从而加快 AI 应用的开发速度。

4. 集成 IPFS 分布式存储

去中心化应用需要使用文件存储系统来存储数据，一个选项就是 IPFS 的存储系统来替代传统的中心化云存储或者本地文件存储，从而实现更好的分布式存储。

IPFS 星际文件系统（InterPlanetary File System，缩写 IPFS）是一个旨在创建持久且分布式存储和共享文件的网络传输协议。它是一种内容可寻址的对等超媒体分发协议。在 IPFS 网络中的节点将构成一个分布式文件系统 [2]。未来的 IPFS 大部分会使用跨链技术调用，关于跨链技术，请见跨链服务调用。

5. AI 工程师培养中心

Nebula AI 将建立系统的人工智能培养中心，提供人工智能实践领域的基础知识，工程师们通过系统学习，项目实操，逐步在产品设计中建立和训练人工智能模型。我们致力于传播人工智能行业最新应用和知识、培养输送优秀人工智能人才。以填补人才缺口、充分发挥人工智能在商业中的力量为使命。

2 智云链生态系统

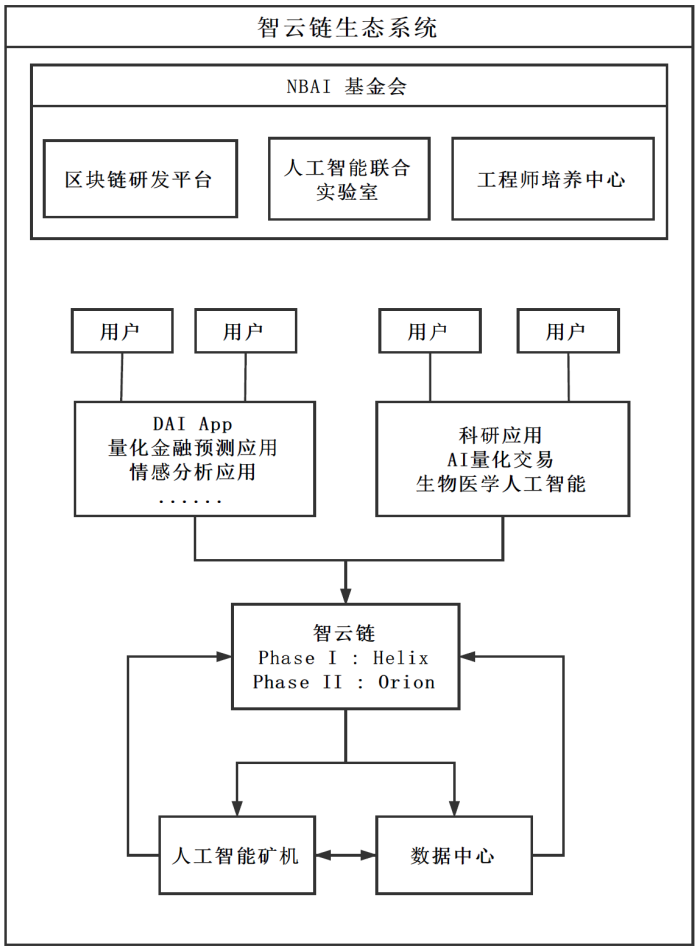

图 1: 智云链生态系统

智云链生态系统主要由两部分构成，NBAI 基金会与智云链系统。NBAI 基金会支持资助区块链研发平台、人工智能联合实验室以及工程师培养中心的发展和运营管理。智云链系统则集合了 DAI App、科研应用及高校教育等顶层应用，智云链区块链，以及人工智能矿机和人工智能数据中心的底层支持。

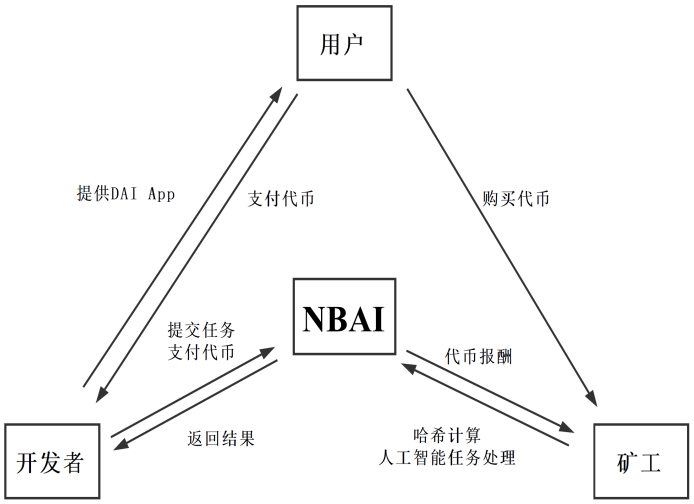

图 2: 经济模型

智云链生态系统的经济模型如图 2 所示。开发者向用户提供 DAI App，用户根据开发者制定的规则支付 NBAI 代币或免费使用 App。开发者向 NBAI 提交人工智能任务，并根据 NBAI 预估的费用支付 NBAI 代币，之后 NBAI 将任务公开，矿工自由从智云链接收并处理任务，完成任务后矿工获得相应 NBAI 代币作为报酬。用户与矿工之间可以通过交易所进行 NBAI 代币交易，从而实现了一套完整的价值流转增值经济模型。

2.1 智云链

在智云链系统中，有大量的人工智能深度学习的模型（如 RNN，CNN 和 LSTM）训练，需要大量的 GPU 运算来完成。为了解决这个问题，我们必须改变区块链挖矿方式，不再单纯以工作量证明（PoW）为解决方案，而是采用初期 PoW 后期群体工作证明（Proof of Group) 的方式发放代币。现有的矿机可以进行人工智能计算来获得代币回报。在初期仍然使用 Ethash 作为工作量证明（PoW）方式保证出块的稳定性，但是中期将启用群体工作证明（PoG）来完成。

2.1.1 Helix (PoW)

在白皮书发布的同时，一个加载智能合约的人工智能独立公链将发布。因此项目的第一阶段将使用独立的 ether 链实现。独立的 ether 链有以下优点:

- 较少的流量延迟
- 自定义的 gas

  有利于激励矿工通过智能合约获得收益，而不是依靠智能合约的 gas 收益。
- 自定义的难度

  可以提高出块速度，调整代币生产的速度。

每个人工智能节点根据计算能力的不同，可以通过智能合约取得任务池里的任务进行计算，在提交结果后获得代币回报。智能合约的 hash 会记载在块中用于标识任务的地址。合约中会设定任务地址和工作量以及工作费用。

然而，目前比特币已经吸引全球大部分的算力，其它使用 PoW 共识机制的区块链应用已经难以获得足够高的算力来保障自身的安全。挖矿造成大量的资源浪费，必将导致环境破坏能源短缺，致使全人类都需要为之买单。区块的确认时间难以缩短，达成共识的周期较长，已经不适合现阶段流行的商业应用，且 PoW 共识机制对均衡攻击尚无解决方案 [7]。综上所述，我们认为智云链生态系统需要应用一套全新的共识机制来解决工作量证明存在的潜在漏洞和优化智云链的共识机制。

2.1.2 Orion (PoG)

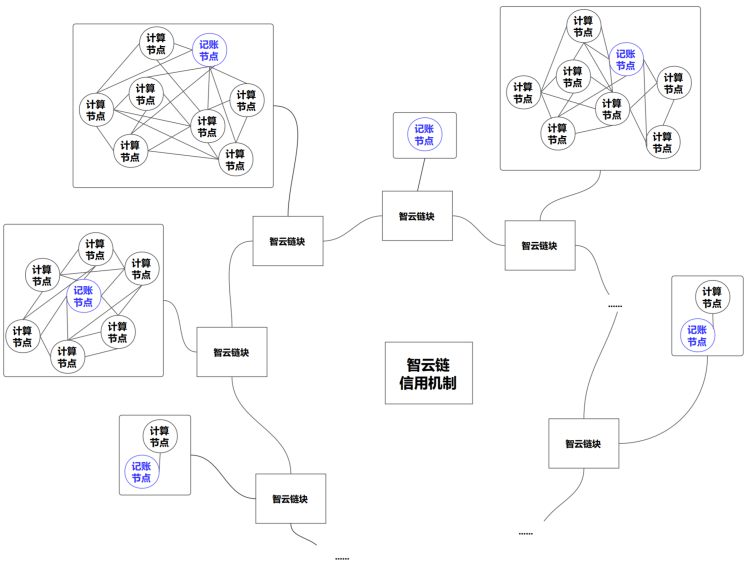

图 3: 智云链 PoG

由于人工智能的训练数据非常庞大，在系统内拿取数据的时间会变得非常的关键，云计算的特性则是节点之间的距离越近通信的成本越低，相应的计算的效率就越高。根据这个特性以及对 PoW 共识机制现存问题的思考，我们将使用一种新型的群体工作证明（Proof of Group）。在 PoG 中我们将结合使用共识系统和智云链信用机制来保障效率与安全。

我们给出如下定义：

定义 1 工作节点与记账节点

工作节点是主要的人工智能计算任务执行节点，它的主要作用就是用来执行人工智能运算任务。

记账节点除了普通的计算功能还可以负责管理其他节点和记账的功能。当 AI 任务需要分布式执行时，记账节点负责分配任务给本区域所有的 node 执行，任务执行结果写入 IPFS，而任务完成的合约则由记账节点通过拜占庭共识提交主链进行验证。

当一个新工作节点加入系统时，他将首先广播搜索周围的节点。

- 发现了周围节点的响应时间在时间 t 内，
  选择加入周围的节点网络成为其中一个 worker。
- 周围没有任何节点的响应时间在时间 t 内，
  自己被选举成一个记账节点。

定义 2 如何成为记账节点

在一个节点网络内，工作节点成为记账节点的方式有两种：

- 如果网络内原记账节点消失，那么信用最高的节点自动成为记账节点。
- 假设节点网络中有 n 个工作节点，记为 P，各节点在节点网络中的生存时间为 t，若 $\exists p_i$, 其与网络中其他所有节点之间的响应时间和 $\sum_{i=1}^{n-1} T$ 与其自身的生存时间 t_i 的乘积最小，则该节点为记账节点。

定义 3 虚拟工作组

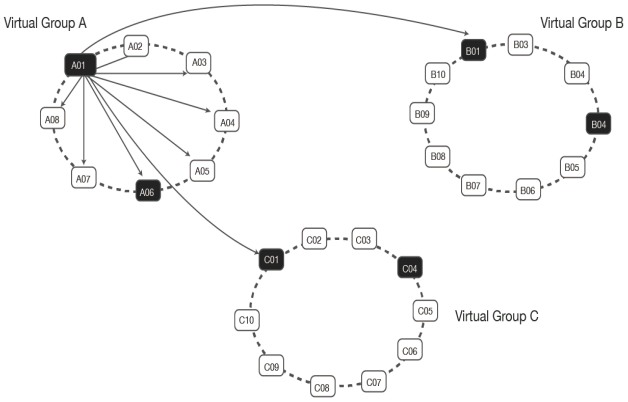

图 4: 虚拟工作组

若干的工作节点会合成一个工作组。工作组中的备份系数定义为可以同时记账的节点数，假设一共有 n 个节点在节点中，则备份系数可以为 $1 < k < n + 1$; 当 $k = n$ 时，则转变为 Helix 系统。备份系统是一种在组内保持账本的一种方式。然而矿工为了尽量获得挖矿的收入，可能会人为试图调高备份的系数 k，对此，系统设计成主要收入来自于 AI 计算，挖矿产出应该是低于 AI 节点的运算收入。

定义 4 组间通信

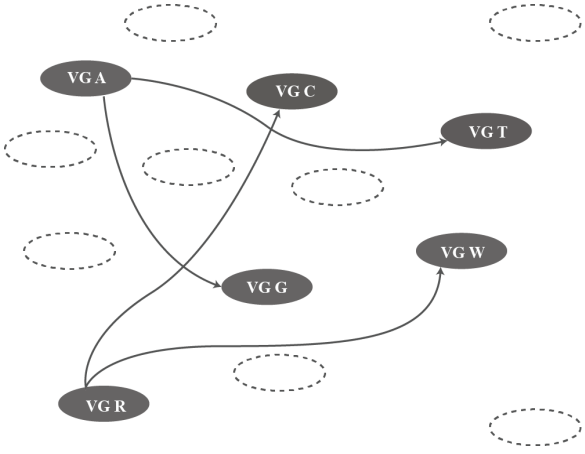

图 5: 组间通信

工作组之间共同组成了一个记账网络，该网络使用拜占庭共识系统进行联合记账 [10]。充分保证了防止 51% 攻击和记账效率之间的平衡。

在 Nebula AI 提出的群体工作证明（PoG）中，每个参与者，记为 P_i ，都需要在区块链网络中知道其认为重要的其他人，记为 Pk_j。一笔交易结算，记为 TS，

需要等待所属群体内绝大多数其他人就以前的任何交易达成一致。

假设 $P_i, Pk_j \in$ 群体 G，共识算法 $Consensus(A, B)$，共识验证算法 $Verify(V, NL)$，那么，每个节点共识计算为：

$$\forall i \quad TS(P_i) = \prod_{j=1}^{n} Consensus(Pk_j, P_i) \tag{1}$$

更进一步，那些被认为重要的参与者被认可只有当他们认为重要的参与者同意，依此类推，在群体工作组中，最终达成共识的计算为：

$$TSA = Verify(\frac{\prod_{i=1}^{n} TS(P_i)}{Consensus(G)}, [P_i, Pk_j]) \quad P_i \in G \cap Pk_j \in G \tag{2}$$

最终，当拥有足够的网络节点，系统将接受这笔交易，且这一系列分层的群体共识使得攻击者无法拥有完整共识信息，从而无法实现攻击。只有这样，任何参与者才会考虑交易入驻。PoG 共识可以确保人工智能任务以及交易信息的完整性。

2.1.3 任务的执行

任务池包含两种任务：

- 系统生成任务。例如 Ethash，蛋白质测序等，标准单位回报。
- 用户任务。用户为解决某些问题提交任务，用户会设定任务回报。

无论哪种任务都会附带一个小型的智能合约统，用于将合约以及计算结果提交。挖矿将同时获得任务回报和记账回报。

一个标准的训练任务包含以下内容：

- 任务使用的训练数据。数据集可以来自 foundation 提供或者自定义。
- 任务使用的训练脚本。训练方法来自于标准的深度学习模型（RNN，CNN，LSTM 等）以及其他自定义方法。
- 训练报酬。训练任务由 AI 矿机完成，需要指定报酬的数量，越高的费用会提高训练的优先级。

任务系统存储在集成 IPFS 上，用于存放运算加密后的算法代码以及任务代码。

当矿机接受到计算任务后，会返回本身的硬件参数，从远程下载计算任务单元以及训练数据集。标准的 Distributed TensorFlow 进行封装后，加入适当的冗余计算以保障计算结果的可靠性。

2.1.4 跨链服务调用

作为去中心化的人工智能系统，很多组件都将是去中心化的，然而全部自行设计开发是非常低效的，系统应该是与其他去中心化服务联通并且可以方便的跨链使用。跨链分为两种：价值跨链与技术跨链。

价值跨链是通过去中心化交易所实现跨链交易，例如在以德上通过智能合约交换得到所需的服务的代币，然后使用这种代币驱动相应的服务进行。该技术简单易行但是性能低下。但是如果在系统中提前兑换好服务需要使用的代币就可以降低延时。在目前条件下 USDT、比特币都会是典型的价值跨链媒介。

技术跨链的案例有比特币与莱特币的跨链原子交易达成，采用 Segwit 隔离见证，不同币种之间可以进行跨链交易。此外，Zcash 和以太坊之间正在进行零知识验证交易，零知识证明使 Zcash 代币成为不可追踪的，通过在公共 Zcash 区块链上创建私人交易。一个底层链需要被设计出用于跨链交易。目前已有大量的 ICO 项目在进行跨链方面的尝试，例如 Ethcore 公司在跨链通信领域的 Polkadot 项目，其设计核心理念为解决两大阻止区块链技术传播和接受的难题：即时拓展性和延伸性。该项目目前以以太坊为主，实现其与私链的互联，并以其他公有链网络为升级目标，在其技术成熟之后集成会极大提高项目的适用范围和性能 [5]。

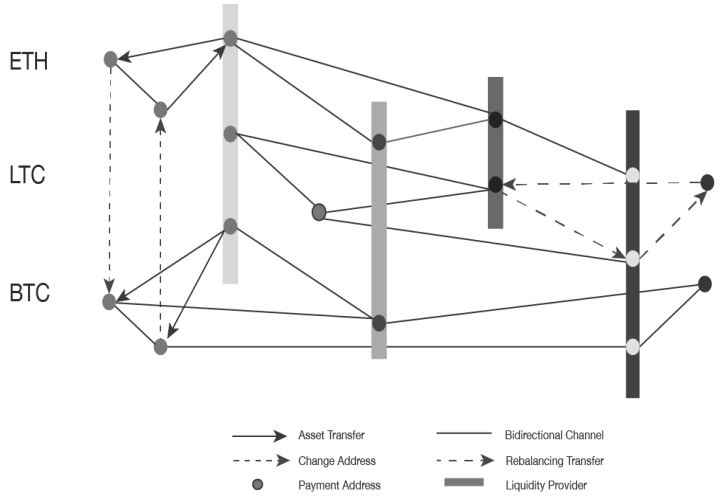

图 6: 跨链服务调用

2.2 人工智能数据中心与矿机

2.2.1 人工智能数据中心

为了在大规模的用户加入之前保证一定的 AI 算力供应，我们位于将与魁北克的大规模的第三方互联网数据中心合作，为人工智能挖矿计算提供初期的算力。魁北克具有全球极具竞争力的电费，寒冷的气候，充足的人才以及多达 34 个数据中心。此外，世界著名的大公司包括 IBM，诺基亚，亚马逊，微软的数据中心机房均建设在此地。

魁北克作为人工智能数据中心的优势：

- 充足的水资源与低廉的电费。

表 1: 魁北克电费水平

Province	375 kWh	750 kWh	1,000 kWh	2,000 kWh	5,000 kWh
Quebec	32.48	52.77	68.66	146.46	379.86
Manitoba	34.03	60.96	78.92	150.75	366.24
British Columbia	32.05	61.92	89.07	197.63	523.34
New Brunswick	52.88	88.32	111.94	206.44	489.94
Alberta	57.775	96.175	121.78	224.195	531.44
Saskatchewan	61.955	103.685	131.505	242.79	576.65
Ontario	64.7	110.64	141.69	267.34	674.38
Nova Scotia	64.69	118.55	154.46	298.09	728.98

  据 Ontario Hydro 和 Hydro Québec 2013 年的统计数据显示，加拿大拥有全球最低廉的电费，在加拿大的所有省份中，魁北克的电费又是最低 [16]，且 90% 以上使用水电站能源。

- 较低的气温

  魁北克有长达九个月的冬季，且冬季平均气温低于零下十度，即使在夏季平均气温也低于二十度。低温让机房的散热耗能大大下降。

- 充足的人工智能的人才储备

  谷歌、脸书、微软均在蒙特利尔设立了人工智能中心。这里汇聚了大量的人工智能领域的人才。比如蒙特利尔大学计算机科学与运筹学系的约书亚 · 本吉奥（Yoshua Bengio）教授就是世界顶级人工智能研究学者，他是蒙特利尔学习算法研究所的负责人，高级机器学习在人工智能领域的三位奠基人之一。

此外加拿大政府也对人工智能的研发给予充分的支持。联邦政府总已给蒙特利尔大学特批 2.13 亿加元的经费，同时省政府也计划在未来五年内追加 1 亿加元的投资。

- Nebula AI 已经与世界一流学府麦吉尔大学医学院达成 AI 方面的联合研发合作，致力于研究人工智能在外科方面的创新应用。

2.2.2 人工智能矿机

一张 1080Ti 显卡的计算能力为 7514 GFLOP/s。在 GTX 1080Ti 上使用 Caffe 框架训练 130 万条图像数据的 GoogLeNet 模型，迭代 30 次的计算时间为 19 小时 43 分钟。六卡并行计算的时间可以缩短为 3.5 小时。

任何支持 CUDA 运算（主要为 Nvidia 系列显卡）的 GPU 矿机均可安装 AI 挖矿系统。AI 矿机上预装了常见的人工智能算法，如 CNN，RNN，DNN 等，以及大量其他常用的库，如 TensorFlow 等，系统附带的升级客户端可以自动对 AI 预装支持库进行更新。第一批计算矿机将主要预装 python 3.6 支持库。支持 Ethash 的记账客户端也跟系统一起集成。

在 AI 矿机上可以获得三种收入：

- 记账运算收入
  以 Equahash 为基础的算法支持记账部分收入。但该部分收入一般小于 AI 计算的收入。
- AI 计算收入
  AI 的计算收入为矿工最要的收入来源。
- IPFS 收入
  矿机可以开启双挖模式，支持 Sia，storj 类型的文件共享币种挖矿。IPFS 同样可以用于支付 AI 计算中存储数据之用。

2.3 DAI App 开发

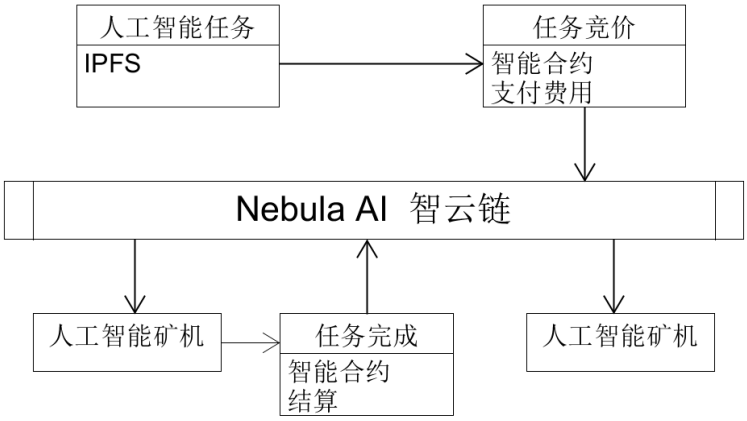

图 7: 人工智能 DAI App

以太坊社区把基于智能合约的应用称为去中心化的应用程序（Decentralized Application)。DApp 的设计目标是让智能合约有一个友好的界面，外加一些额外的功能，例如 IPFS。DApp 可以在一台能与以太坊节点交互的中心化服务器上运行。例如著名的 etherdelta, 以太猫等等。

然而对于去中心化人工智能应用程序 (DAI App)，仅靠目前的智能合约是不够的。原因有以下几点:

- 以太坊智能合约并不带有人工智能计算功能
  EVM 是一个图灵完备的合约虚拟机，但是其共识计算系统只能执行简单的任务，无法执行复杂的人工智能计算。
- 以太坊挖矿客户端也不支持人工智能计算所需要的计算库
  人工智能的运行很大程度上取决于各种开发包的支持，分布式计算是其主要任务。相关计算任务所需的支持库可以用单独的计算客户端实现。

然而作为一个商业化可用人工智能应用，区块链的超级账本以及支付功能仍然是系统的核心部分。且由于人工智能计算资源的稀缺性，共享计算能力将成为一个非常有用的功能。每个用户均可链接到链上利用区块链租借计算能力完成计算任务，每个 DAI App 的开发者根据自身的需求，编写出符合标准的智能合约。

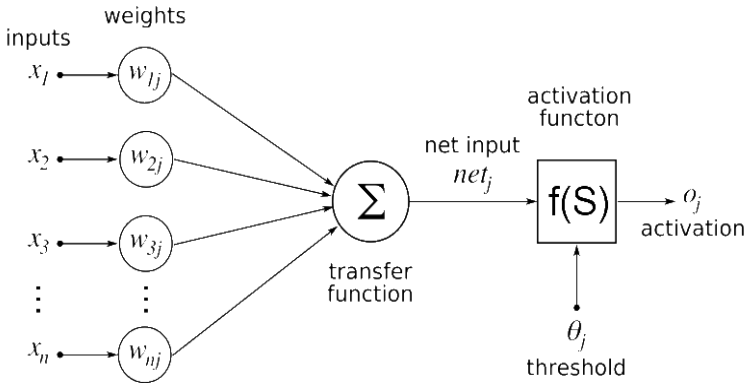

图 8: 深度学习

在训练深度学习模型时，将执行两项主要的操作：正向传递和反向传递。在正向传递中，输入通过神经网络并在处理输入后生成输出。而在反向传递中，需根据正向得到的误差来更新神经网络的权重。在神经网络的训练过程中，一个最重要的问题就是训练速度，特别是对于深度学习而言，参数的调整会消耗大量的时间。神经网络的计算密集部分由多个矩阵算法组成，而 GPU 在矩阵运算和数值计算方面具有独特的优势，特别是浮点和并行计算的性能上能优于 CPU 数十到数百倍。在使用 GPU 训练深度学习模型时，还能便于在云端进行分类和预测，从而在耗费功率更低、占用基础设施更少的情况下能够支持远比从前更大的数据量和吞吐量。因此，通过智能合约获得足够多的计算能力进行人工智能计算是一个行之有效的手段。

我们以典型的风格转移深度学习模型（Gatys et al.）为例，比较 GTX 1080 Ti GPU, K80 GPU (AWS P2), i5 7500 CPU 和 CPU (AWS P2) 运用 tensorflow 框架计算的时间。

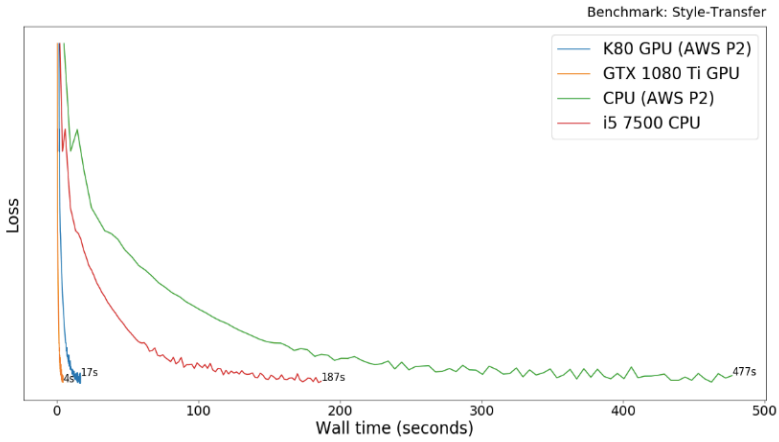

图 9: 速度比较

GTX 1080 Ti GPU 的性能优于 i5 7500 CPU 接近 50 倍。

Nebula AI 能够提供非常具有市场竞争力的计算能力。Nebula AI 的人工智能矿机使用 Nvidia 1080 Ti, 以 Amazon P2.xlarge instance（Nvidia Tesla K80）为例我们做以下计算：Nvidia 1080 Ti 的价格为 1000 加币，每小时电费消耗 0.1 加币，假设一张 1080 Ti 的寿命为两年，其每小时运算单价为 $1000/(36 \times 2 \times 24) + 0.1 = 0.157$ 加币/小时。

通过官方测试数据可知，Nvidia 1080 Ti 的 Tensorflow GPU 性能为 Amazon P2.xlarge instance 的四倍 [14]，而 P2.xlarge 的价格为 0.9 加币/小时，是 Nebula AI 提供的计算能力单价的 23 倍。用户需要将数据上传至 Amazon 服务器进行计算，无法保证数据的私有，使用去中心化的智云链则能解决此问题。

2.4 高校教育

智云链为全球各大高校的科研计算提供丰富的接口，能够极大的提高科研人员的工作效率，降低研发成本，打破跨界多领域高级编程需求与底层配置对接的壁垒。智云链生态系统提供的 PaaS（Platform as a Service）能够使得高校学生抛开不必要的底层配置，更专注于兴趣领域的学习。

2.5 Nebula AI 基金会

Nebula AI 生态系统预期成为一个使用 NBAI 加密货币的生态系统合作伙伴社区。Nebula 基金会旨在成为面向这个生态系统成员的一个独立、非盈利、民主的治理机构。

一个区块链 AI 基金会将成立用于人工智能基础链的推广教育以及创业资助活动。我们鼓励社区任何人的加入和一切愿意将系统集成到 Nebula AI 的平台上的 DAI App 的研发互动活动。

基于独立性原则，社区基金会的钱包采取 3/4 多重签名。若增加签名，需经过财务及人事管理委员会。大额的代币进行冷存储；小额的代币使用多重签名的方式。

2.5.1 人工智能联合实验室

Nebula AI 基金会将于蒙特利尔大学，多伦多大学，麦吉尔大学展开在 AI、区块链、分布式计算方向的广泛合作。加拿大决心在中部的多伦多 — 滑铁卢、东部的蒙特利尔以及西部的埃德蒙顿地区打造新兴的超级人工智能中心，建立完善的资金、业务和人力生态链。在 2017 年，联邦财政公布的政府年度预算亦表明将着重拨款以上地区的人工智能产业，在国家发展政策层面将人工智能提至第一位。

蒙特利尔大学约书亚 · 本吉奥（Yoshua Bengio）教授及团队在过去 10 年中进行的研究，打下了基础，把蒙特利尔推到了人工智能的前线。Bengio 也在蒙特利尔大学的算法研究所（MILA）继续学术研究。MILA 由数据颂赞研究所（IVADO）支持。Nebula AI 正在与 MILA 积极沟通推进合作研发工作。

北美顶尖医学院麦吉尔大学医学院外科创新项目（Surgical Innovation program (Department of Surgery)）与 Nebula AI 开始了一项由 Mitacs 计划支持的 AI 医学影像方向的研发活动。Mitacs 计划是加拿大信息技术与综合系统数学组织发起设立的合作项目，已运行十余年。著名医学教授 Jake Barralet 是该计划的领导人。

2018 年 2 月，在硅谷成立研发实验室与本地的高校、业界就人工智能应用以及区块链研究展开广泛充分的合作。

2.5.2 区块链研发平台

Nebula AI 将组成以 Nebula AI 区块链工程师以及社区贡献者为核心，联合高校科研与业界领先技术等资源的区块链研发平台。同时为区块链工程师培养中心提供技术支持与人力资源。

Nebula AI 的研发平台包括开发样例，开发 API/SDK 接口，在线学习视频，技术支援小组以及多种应用场景实施中心。分布在世界各国的研发人员和社区合作者将共同为 Nebula AI 平台提升功能和易用性。

2.5.3 人工智能与区块链工程师培养中心

每一个成功的项目都离不开大量的工程师。目前市场处于紧缺 AI 人才的阶段。Nebula AI 以资金和项目平台合作的方式，与本地的 ECV learning 等教育机构合作。Nebula AI 的 AI 科学家们也将充当项目讲师，招聘大量的 AI 实习生，持续的为人工智能产业提供高素质的人才。2018 年 1 月 27 日由熊腾科博士主讲的人工智能工程师培养项目成功赢来第一批学员。他们将成为 Nebula AI 未来坚实的研发团队后备力量。区块链培养项目也已于二月中旬开课。

3 智云链架构设计

3.1 智云链逻辑架构

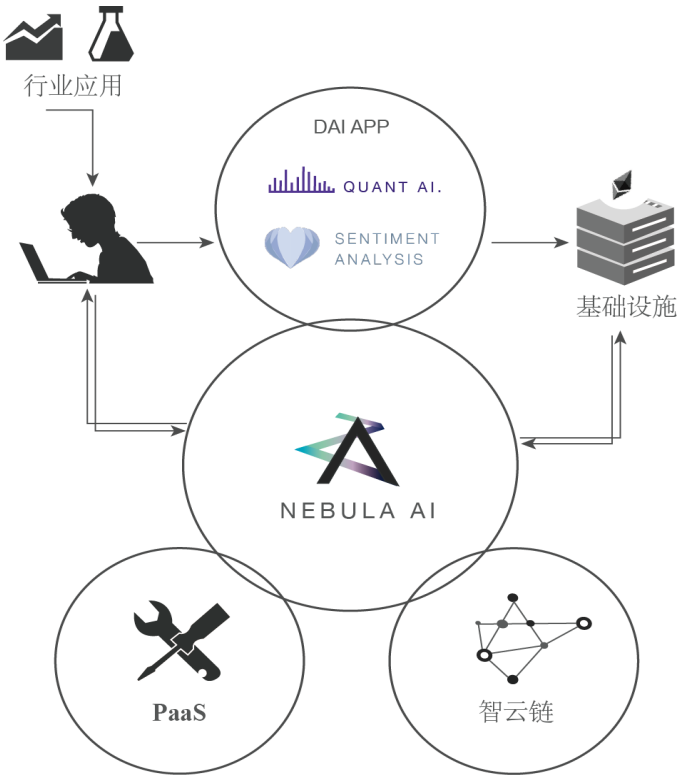

图 10: 系统逻辑图

智云链的逻辑结构主要由行业应用需求、开发者、DAI App、基础设施和 Nebula AI 相互交流组成，其中 Nebula AI 分别提供 PaaS（Platform as a Service）以及智云链区块链。大量金融、医疗、生物等行业的人工智能开发需求，促使开发者根据不同的行业应用需求开发 DAI App，并通过部署应用，加入 Nebula AI 生态系统提供解决方案，获取收益。Nebula AI 将提供丰富的接口和应用，方便开发者的使用。智云链提供的去中心化区块链结合 Nebula AI 的信用机制，将着手解决敏感数据及模型的 P2P 信任和大数据处理的效率问题。

3.2 智云链系统架构

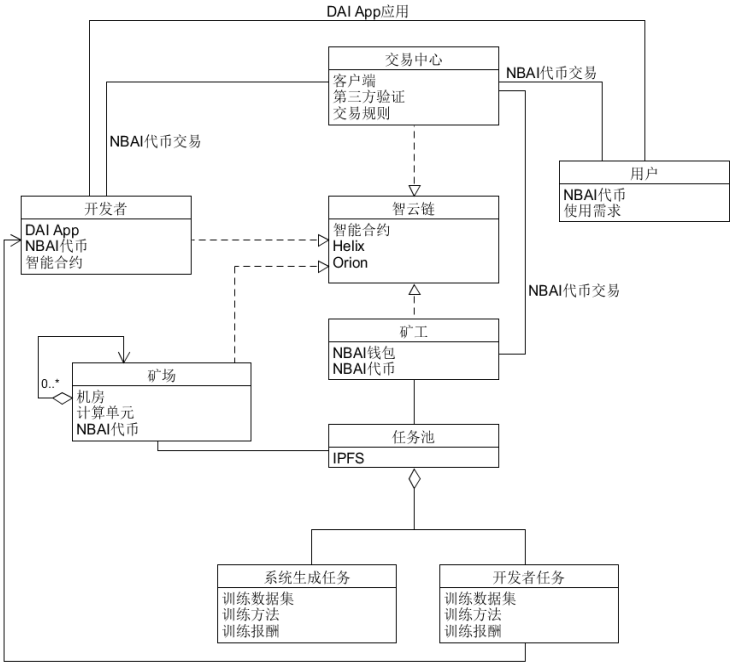

图 11: 系统架构

如图 14 所示，智云链的系统架构主要由智云链、开发者、用户、交易中心、矿工和任务池等构成。Nebula AI 不仅提供了去中心化的智云链区块链，还提供了 NBAI 代币交易中心，用来完善价值在智云链生态系统中的传递。

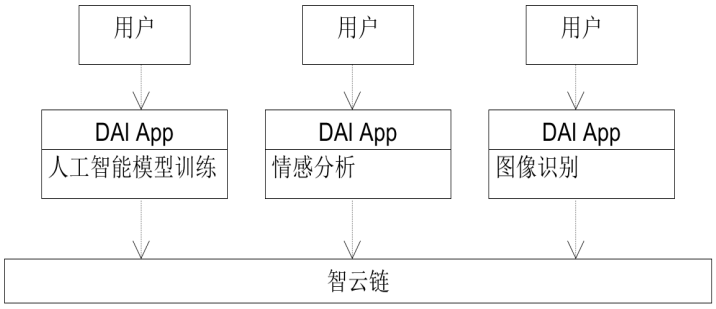

图 12: 共享 AI 云计算平台

Nebula AI 提供了共享 AI 云计算平台，PaaS（Platform as a Service）更是能让非 IT 领域的细分行业从业者实现快速开发部署，减轻对系统环境以及计算能力的依赖。

3.3 API/SDK 支持

一些常见的预付或追加费用的智能合约可以用 SDK 程序化地生成接入，API 则是在某个中心化服务里提供接口。第一批支持的 SDK 将是 python 为主要编程语言，java,.net 将陆续支持。

有了 SDK 的支持，用户可以程序化地驱动 AI 计算，从而为用户提供更多的便捷性，并且使用户成为与中心化系统的一个接口点。

4 智云链优化设计

4.1 数据安全加密

数据的保存将使用同态加密方案 (Homomorphic Encryption) 进行存储，秘密同态的思想是指：对几个数据的加密结果进行运算后再解密，得到的结果与这些数据未加密时执行某一运算所得的结果一致。目前出现的同态加密方案可被分为三种类型：部分同态加密、浅同态加密和全同态加密。部分同态只能实现某一种代数运算（或、乘、加）；浅同态能同时实现有限次的加运算和乘运算；全同态能实现任意次的加运算和乘运算。同态加密方案除了可以实现加密功能外，还可以用于密文数据的计算。

设 $< G, * >$ $< H, o >$ 是 2 个代数系统，$f : G \to H$ 是一个映射，如果对于 $\forall a, b \in G$，都有 $f(a * b) = f(a) o f(b)$，则称 f 是从 G 到 H 的一个同态映射。加密是从明文空间到密文空间的映射，如果加密映射是一个同态映射，我们就说它是一个同态加密方案。或者说同态加密是加密运算和某一代数运算或者混合代数运算可以交换顺序的加密方案 [20]。我们给出如下定义：

设 $E(K, x)$ 表示用加密算法 E 和密钥 K 对 x 进行加密，F 表示一种运算，如果对于加密算法 E 和运算 F，存在有效算法 G 使得：

$$E = (K, F(x_1, ..., x_n)) = G(K, F, (E(x_1, ..., x_n))) \tag{3}$$

就称加密算法 E 对于运算 F 是同态的。

如果定义中的等式仅对 $F(x_1, ..., x_n) = \sum_{i=1}^{n} x_i$ 成立，那么该加密方案就是一个加法同态加密方案。

如果定义中的等式仅对 $F(x_1, ..., x_n) = \prod_{i=1}^{n} x_i$ 成立，那么该加密方案就是一个乘法同态加密方案。

如果定义中的等式对包含加法与乘法混合运算的 $F(x_1, ..., x_n)$ 成立，那么该加密方案就是一个全同态加密方案。只对一种运算成立的同态加密方案称为部分同态加密方案。

公钥体制的同态加密方案 ε 由 $KeyGen_\varepsilon$, $Encrypt_\varepsilon$ 和 $Decrypt_\varepsilon$ 这 3 个随机算法组成。

- $KeyGen_\varepsilon$：接收安全系数 λ 作为输入，输出私钥 sk 与公钥 pk，pk 定义了明文空间 P 和密文空间 X。
- $Encrypt_\varepsilon$：接收输入 pk 和明文 $\pi \in P$，输出用公钥 pk 加密明文 π 所得的密文 $\psi \in X$, 记作 $\psi = Encrypt_\varepsilon(pk, \pi)$。
- $Decrypt_\varepsilon$：接收输入 sk 和 ψ，输出明文 π。

上述 3 个随机算法的计算复杂性都由 λ 的多项式所决定。且加密系统应满足正确性条件：即如果 $(sk, pk) \xleftarrow{R} KeyGen_\varepsilon(\lambda)$，而且 $\pi \in P$，$\psi \xleftarrow{R} Encrypt_\varepsilon(pk, \pi)$，那么 $Decrypt_\varepsilon(sk, \psi) = \pi$。

此外，$Evaluate_\varepsilon$ 算法被解释为：输入公钥 pk、从电路集合 C_ε 中选取的一个电路 C 以及一组密文 $Y =< \psi_1, ..., \psi_t >$，输出密文 $\psi \in C$。如果：

$$\psi_i = Evaluate_\varepsilon(pk, \pi_i), i = 1, ..., t,$$

那么

$$Evaluate_\varepsilon(pk, Y, C) = Evaluate_\varepsilon(pk, C(\pi_1, ..., \pi(t)) \tag{4}$$

一旦运算法则被保留下来，那么数据结构也会随之被保留下来。因此在机器学习的过程中，我们只需要数据结构，就可以对加密信息进行解密和机器学习。

4.2 分布式系统优化

通过对大数据进行等值分割处理能够加速数据的传输，智云链上的工作节点收到任务进行并发处理，之后各节点将结果返回至选定的聚合处理节点进行任务的合并，最后返回任务所有者。在这些传输与处理过程中，我们将通过对节点选举、数据存取、负载均衡、网络安全及冗余机制的研究对智云链进行优化。

当智云链从开发者接收到大数据级的人工智能任务后，单个矿工无法独自处理任务，我们需要将任务进行拆分并交付给多个矿工进行计算，并最终通过任务聚合返回给开发者最终结果。这一系列操作需要依赖于完备且优化的分布式系统设计。智云链也将在满足高吞吐、低延迟和高并发等性能需求方面做出优化。

虽然传统的分布式系统结构仅有三层，但是根据业务需求，往往会被设计成更多层次。一个多层结构常常会具备各种各样的代理进程和路由。这些代理进程之间，大多应用是通过 TCP 来连接前后两端。然而为了避免 TCP 的高故障率及高维护开销，智云链将应用消息队列机制实现进程间通讯。 智云链使用 NoSQL 来实现数据存储层的分布的解决方案。NoSQL 除了高承载量和高速访问的优势外，它只能使用一条索引来检索和写入。这种约束带来了分布式实现上的优势，系统可以按这条主索引定义数据存放的进程。这样一个大数据级别的任务数据，就能安全地发送到不同的节点。

```
future<int> get();
futre<> put(int);

void function(){
        get().then(then[] (int i)){
                put(i + 1).then([] {
                        std::cout ”an integer has been put”;
                        });
                });
}
```

图 13: Future/Promise 模型

由于分布式系统涉及非常多的网络通信，且系统实现依赖于异步非阻塞编程模型，开发人员在对分布式系统的编程中会生成大量回调函数。任务指令会被分散到多个进程，通过多次网络通信组合完成。然而，回调这种异步编程模型非常不利于代码维护。为了解决这个问题，智云链应用 Future/Promise 模型进行了回掉函数集中优化。

5 智云链代币 NBAI

5.1 代币方案

5.1.1 代币的使用价值

系统的代币用于购买计算能力，当训练数据比较小的时候，消耗的代币比较少，当训练数据大的时候消耗的代币相应增多。支付的费用与训练成本和当前代币的价值有关。为每个 1080Ti 的显卡计算一分钟产生的计算能力，也就是 7514 GFLOP/s $\times$ 60。

5.1.2 代币的应用场合

代币会在以下三种情况下使用：

- 开发者测试

  开发者在测试中会消耗一些代币用于模型的训练。根据支付的代币的多少，训练模型所需的训练时间会减少 50% 90% 不等。

- DAI 应用的使用

  DAI App 可能被开发者设置成付费 app，则使用者必须付代币才能使用这些人工智能服务，比如本白皮书中的预测数字货币走势 app。

- DAI 训练服务购买

  在用户使用训练服务来取得更精细的模型时，可能会被要求支付训练费用才可以重新训练模型。

5.1.3 用户使用场景

1. 量化交易

量化交易从很早开始就运用机器进行辅助工作，分析师通过各种量化模型，设计一些指标，观察数据分布，将机器当做一个运算器来使用。直到近些年机器学习的崛起，数据可以快速海量地进行分析、拟合和预测，从而更加精确预言未来金融产品的行情走向，然而这些模型的计算需要大量的人工智能计算能力。如果采用传统的方式，每个交易部门都需要自行建立一套数据中心。而共享计算能力可以省去

昂贵的维护费用。让金融交易公司更加专注于预测本身。

2. 人工智能学习者计划

高校目前开始逐渐开设人工智能课程，这种趋势在未来几年将会更加流行，学生学习的时候一般会选择在本机运行小任务，在学校机房运行耗时的任务。然而这些碎片化的任务，完全可以用区块链算力云解决。低成本的 AI 计算服务非常适合学生完成各种运算练习，快速修改自己的模型。

3. 生物医学人工智能

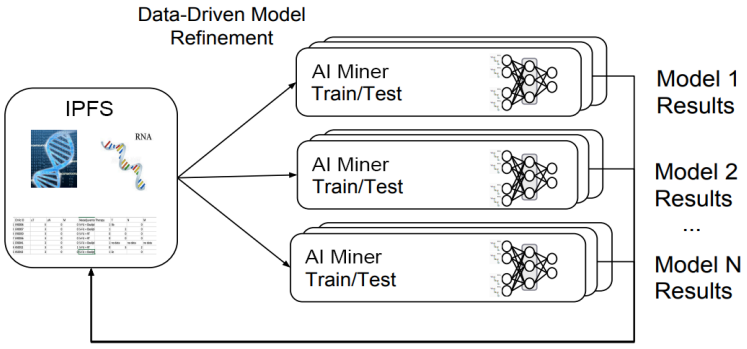

图 14: AI 用于肿瘤研究

肿瘤的早期筛查意义重大，但由于早期癌症病变区域小，传统方法难以判断良恶性，给临床诊断造成了困难，医生往往需要通过活检的方式进行检测，不仅增加了医疗成本，也给病人带来巨大痛苦。而将人工智能运用于医学影像识别和多学科协作诊断，可以有效突破这一难点，提高医生诊断能力、帮助快速决策，促进医疗服务向个体化、精准化转变。

5.2 DAI App 开发者收益模式

1. DAI App 任务类型

- I 类 DAI App — 需要训练模型的 App

  这一类 App 用户必须支付代币来驱动运算，运算需要消耗大量的资源。训练时间根据任务的不同可能需要几小时甚至几百小时。

- II 类 DAI App — 无需训练模型或使用已有模型的 App

  无训练模型的 DAI App 无需消耗计算能力，只需要支付一定的智能合约费用

即可应用。也可以调用 I 类 DAI App 模型计算结果来生成应用。这一类 DAI App 的开销比较低。

2. 计算任务

一个标准的算力支付合约将包含以下基本元素:

- AI 任务的数据地址
- AI 任务的程序脚本
- AI 任务执行结果输出地址
- AI 任务的报酬

3. 任务发布

当任务发布在链上时，所有的 AI 矿机都可以从系统中接受任务。任务被矿机执行时会被标识成 “进行中” 的状态，用户可以设置几个不同等级的冗余计算以保证更高正确率的结果。Nounce 可以设置为 1，2，3 等不同级别，以对应不同的冗余计算度。数字越大意味着需要更多的计算来保证计算结果的准确性。相应的费用也会更高。

4. 费用计算

AI 计算一般分为训练阶段和使用阶段。在训练阶段将使用大量的训练资源，绝大部分算力将在此处被使用。而在使用阶段，由于训练的结束，将消耗较少的算力。在任务启动时，智能合约会预先收取一部分的预付开销，在计算结束时，将再次计算总开销，同时需要客户再次付清余款以取得数据。

为了保证交易的正常进行，用户需要有一定的保证金数额才能开始预约服务，多重签名的自动合约将锁住双方的资金以保证交易的正常进行。

5. 任务执行

矿机客户端从链上读取任务方案，并且解析成可执行的人工智能代码。人工智能和训练用数据可以存放于外部的链接中，当任务开始执行时。会按照以下方案执行代码:

- 解析加密任务
- 远程下载数据

- 将任务设置为执行状态
- 写入运算的进度和结果
- 矿机绑定地址获得回报

6. 计算结束

DApp 的使用者下载执行结果，可以直接用于 web 的展示或者离线使用。执行结果可以使用 API 方式获得，解密后使用。

5.3 智云链 AI 应用案例

对冲基金、银行以及像 Goldman Sachs 一样的大型国际公司正在从基于智能技术的外汇和股票交易中获益。这些公司通过 “深度学习 (Deep learning)” — 可以不断发展演化的数学统计的预测模型和概率模型 — 来预测各种金融市场的短期和长期效果，而像 Pantera Capital 的加密货币玩家、桑坦德银行和花旗银行这类金融机构也在观察如何从加密货币市场中获取利润。

在深度学习模型的设计、搭建、训练和优化过程中，需要大量的计算能力，而每个用户在每次进行参数调整时都需要进行模型的运算。那么在此时，通过智能合约来获得足够多的计算能力进行人工智能的计算则是一个行之有效的手段。

标准的系统流程如图 17 所示:

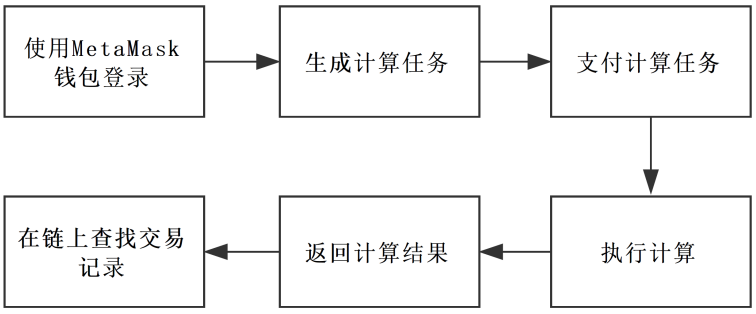

图 15: 智云链 AI 应用流程图

6 发展规划

Q1 2017　概念设想，研发开始，超级账本实现探索。

Q3 2017　人工智能 DAI App 开发，概念原型开发。

Q1 2018	代币销售开始，Helix 测试链上线。
Q3 2018	Helix 公链上线，集成第一个 DAI App； Orion 开发开始，Orion 原型链。
Q1 2019	Orion 测试链上线。
Q3 2019	Orion 公链上线集成 10 个 DAI App。
Q1 2020	Orion 集成 50 个 DAI App。
Q3 2020	Orion 集成 500 个 DAI App

7 合作计划

1. 合作项目

- 分布式优化和云计算项目 — 康考迪亚大学
- 人工智能外科创新项目 — 麦吉尔大学医学院外科创新中心; Mitacs
- 加拿大暑期实习项目 — 加拿大政府

2. 合作伙伴

- 蒙特利尔青年协会
- 加拿大科学与研发基金会
- 麦吉尔大学
- 康考迪亚大学
- Timechain
- Beepay
- Express Mining
- ECV Learning
- 佳林信息技术有限公司
- 蒙特利尔 IT 协会（APIGM）

8 ICO 模式

初始发行 67 亿代币，每年挖矿新生成的代币产量一定，从每年 2% 在六年内递减到 0.2%。适度的当用户使用人工智能的自定义预测功能，此功能将消耗代币，代币的使用量与计算量有关。随着系统的精度的提高，对代币的需求会直线上升。

矿工通过挖矿可以获得代币，人工智能矿机为获得挖矿回报的主要来源。NBAI 数字币是基于 NBAI 区块链的任何应用（例如量化交易、生物智能计算）的唯一支付币种。

代币为 ERC 20 代币，未来将用 Nebula AI 主链代币 1:1 置换。

公募轮 1 Ethereum = 100,000 NBAI。

ICO 软顶：5,000 ETH。

私募开始时间：2018.01.22，结束时间：2018.03.30，私募轮硬顶: 18,000 ETH。

公募开始时间：私募结束后一个月内，公募轮硬顶: 12,000 ETH。

私募未售出的 NBAI 代币将会与公募合并。

公募轮未售出的币将全部销毁。

45% 私募与公募售出

25% 基金会和社区持有

15% 核心团队持有

10% 早期投资者持有

5% 市场合作伙伴持有

私募与公募的投资者不存在代币 NBAI 锁定期。

基金会持有的 NBAI 在众筹结束后处于冻结状态，分 18 个阶段（约 3 年）解冻，每 60 天为一个周期，每次解冻基金会持有量 1/18。

公募结束后将陆续上线国际前几大平台。

代币销售联系邮箱 tokensale@nebula-ai.com。

9 核心团队

9.1 研发团队

NBAI 的项目自从 2017 年初开始筹集验证，经过了多次的技术修改演进，从初期使用 hyperledger Fabric，演进到比特币，最终决定使用以太坊技术作为主干链，历时一年，在此过程中获得来自美国、中国、新加坡、加拿大多国投资人的投入协助。

曹滔韬　CEO & 联合创始人

2007 年毕业于复旦大学电子工程系本科，就职于上海航天，IBM 上海，2010 年赴加拿大获康考迪亚大学获得电子与计算机硕士学位。就读期间获得 NSERC（加拿大自然研究基金）从事视频转码之间的研究。

毕业后就职于加拿大 SAP，Autodesk，Expedia，Paysafe（39 亿美元被黑石集团收购）直至核心项目组长。

2013 年成立 Service ECVictor 专注电子平台类软件设计技术，先后投资数家 O2O，医药，教育，电商物流等领域创业公司。从 2013 年开始积极关注比特币区块链的进展，并在社区开展广泛宣传。

2014 年成立蒙特利尔 IT 协会，拥有会员 700 多人，大小活动逾百次，举办多次区块链，人工智能，大数据等前沿技术的普及，研究讲座。

于 2017 年 7 月在加拿大魁北克成立 Express Computing Inc 以太币挖矿公司。算力销售网站，并同期上线运营，上线三小时即完成数千美金算力销售。该公司矿机设计，挖矿，销售一体化运营。

常年活跃于北美区块链社区，分析多个 ICO 产品。致力于北美区块链的教育普及以及深度研究。

林钦辉　项目经理

在初创和银行业有超过 13 年的咨询和开发经验。他曾是住宅社区初创公司的首席技术官，领导一个团队建立稳固，高并发和可扩展的社交门户，该门户拥有 300 万注册用户。此外，他为富国银行 Wellsfargo，通用资本 GE Capital 和 Laurentian Bank 等银行机构提供超过 7 年的咨询和开发服务，并与利益相关方密切合作，为复杂的金融信息化提供技术解决方案。在 Nebula AI，他从事区块链编程，加密货

币挖掘，并与人工智能整合，致力于建立可承载的，高效的区块链和人工智能的生态系统。

熊腾科博士　人工智能架构师

加拿大 Sherbrooke 大学计算机科学博士、博士后；10 年人工智能研发经验。先后任职多家人工智能公司首席科学家。中科院深圳先进技术研究院，访问学者；数据挖掘和商业智能系统专家；在数据挖掘国际顶级会议和期刊上发表论文 6 篇；2012 年厦门 “双百计划” 领军人才。创立自己的人工智能研究公司，负责项目架构与方案设计。

李岩岩　CFO

CFA、加拿大 CPA 准会员，曾就职于贝恩咨询，申银万国和 TQC 投资等大型企业，在中国证券市场和加拿大投资市场积累了多年的实战经验，熟练掌握中国和加拿大的金融和会计领域的知识，是财务管理、税务规划和融资领域的专家。

吕艳萍博士　人工智能架构师

加拿大 Sherbrooke 大学机器学习和数据挖掘博士，深入研究智能优化算法和数据挖掘的应用。后任教于厦门大学，专注于医疗图像特征提取和分析预测，期间获得 863 项目、国家青年自然科学基金、高校博士点基金、省自然科学基因等多项研发基金，指导多名硕士研究生；在国际顶级人工智能期刊《Machine Learning》，《IEEE Transactions on Biomedical Engineering》发表论文多篇。现负责 Nebula AI 的机器学习项目架构和方案设计。

姚璐　人工智能工程师

曾任职香港金融投资公司量化交易分析师，AXA（香港）金融分析师与商业分析师。广州南雪科技公司联合创始人。华南理工大学 “基于人工神经网络的金融风险预警信号研究” 科研项目负责人。康考迪亚大学经济学硕士。具有多年量化金融研究、统计建模与风险管理经验，精通 Python 与 R 语言。现着重研究深度学习和神经网络算法在金融中的应用。

庞通　区块链工程师

康考迪亚大学计算机硕士。全栈工程师，精通 Ethash，DPOS 等区块链算法，负责区块链产品的设计架构以及实施。

张恺谌　人工智能工程师

华南理工大学电子商务专业学士，康考迪亚大学计算机科学专业硕士。精通 Java, Python 与 Javascript 编程，从事工作与研究方向结合了人工智能，区块链与商业智能。华南理工大学《网络营销》教材撰稿人，曾任职金融教育机构区域经理。积累了多年市场营销及管理经验。现着重在语义分析与深度学习等领域的研究。

岳明　人工智能分析师

擅长机器学习研发和算法优化，具有十年图像识别和视频检测算法的工作经验，研发的产品应用于工厂质量视频检测和铁路交通安全监控系统。目前在 Nebula AI 负责人工智能项目的研发和算法优化。

严如华　资深全栈研发工程师

毕业于福州大学，十年以上在南美，欧洲，北美多国从事核心软件开发工作经验。精通 python，nodejs 等编程语言，参与多个大平台软件平台研发设计。擅长性能优化，代码分析。

Alberto Lacerda　前端工程师

Alberto 在 Laureate International Universities 主修计算机科学。他拥有超过 10 年的 IT 领域经验。曾为埃森哲担任软件开发人员，并与 FIFA 世界杯项目合作。目前是 Nebula AI 的前端开发人员。

张驰　区块链工程师

康考迪亚大学计算机硕士。熟练使用 Python, Js, Java 相关技术及框架，曾负责项目后台服务的开发以及维护。目前作为 Nebula AI 的成员，负责开发区块链相关应用。

李岳　区块链工程师

北京邮电大学计算机系毕业。在中国和北美都从事过软件开发工作，精通 Java, Spring 以及多种软件开发平台。现在在 Nebula AI 负责区块链相关开发。

庞宏　Python 开发

毕业于天津大学，康考迪亚大学应用科学硕士学位。熟悉 python, PHP, JS 多种语言以及相关框架，曾任职服务端软件开发。目前在 Nebula AI 专注于区块链技

术的研发与应用。

周品　软件工程师

周品毕业于哈尔滨理工大学，获得计算机科学硕士学位。她在 IT 开发方面拥有超过 8 年的经验。目前，她在 Nebula AI 担任软件开发人员。

曹沂　机器学习工程师

毕业于 McGill 大学，擅长项目管理和数据分析。目前在 Nebula AI 负责 AI 项目统筹，主要致力于医疗诊断预测和人工智能的应用研究。

温晓军　前端工程师

毕业于 Vanier college Software Applications Specialist 专业, 具有两年的前端工作经验, 为不同类型的客户建立了超过 20 个网站。熟悉 HTML/CSS, JavaScript 等前端开发技术。目前是 Nebula AI 的前端开发人员。

沈思迪　产品设计师

美国 Lehigh University 设计专业硕士。多次获得最佳设计师奖项，多年大公司产品设计经验。负责公司所有产品，网站宣传材料的设计以及市场策划活动。

Alecsa Tabisaura　产品设计师

Alecsa 在加拿大蒙特利尔的 CégepMarie-Victorin 主修平面设计专业。她曾是自由设计师为不同公司的项目提供服务。她有丰富的品牌和用户体验设计方面的经验。目前作为设计团队的一员，担任 Nebula AI 的平面设计师。

徐峥　执行助理兼市场部专员

徐峥毕业于中国传媒大学播音主持专业，曾就职于语言教育、旅游等不同领域，积累了多年销售和市场营销经验。目前在 Nebula AI 主要负责行政和市场营销推广工作。

Jessica Boxerman　市场营销专家

多年市场营销经验，活跃于多个欧洲北美社区。负责欧美社区建设，品牌建设以及市场公关。

徐琰　前端工程师

徐琰在北京大学获得学士学位，之后获得了蒙特利尔理工学院的硕士学位。他

曾在 SAP 担任过 Web 开发人员，目前是 Nebula AI 的 Web 开发团队的主要负责人。

王赞　人工智能工程师

康考迪亚大学电子工程硕士。十年以上数据分析经验，曾就职 LG 电子，SK 电子等知名企业。负责 NLP 自然语言识别，数据处理分析以及相关程序编写，长期从事 LSTM, CNN, RNN 等人工智能算法的研究。

Carlos Gonzalez Oliver　区块链工程师

麦基尔大学计算机科学博士生，也是 Delphi Crypto 区块链咨询的联合创始人。他拥有机器学习方面的专业知识以及解决生物工程问题的项目经验，同时专注于区块链在科学理论中的应用。

9.2　顾问团队

Yan Liu　康考迪亚大学云计算及分布式系统教授

康考迪亚大学云计算及分布式系统专家，发表文章数百篇，有九年以上防御系统开发经验，曾于美国 Department of Energy Pacific Northwest National Laboratory (PNNL) 与 National ICT Australia (NICTA) 担任高级工程师。

Thomas Fevens　康考迪亚大学软件工程系教授及副主任

康考迪亚大学计算数学及计算机视觉项目带头人，麦吉尔大学外科创新中心联合主任，带领科研项目致力于基于临床医疗影像的机器识别和协助癌症诊断预测。在乳腺癌分类识别、牙科诊断方面卓有成就。2018 年, Nebula AI 联合 Fevens 教授建立并推动医疗影像的大数据深度学习项目。

林振华博士　人工智能顾问

硅谷加利福尼亚大学戴维斯分校博士后，从事数理统计研究。2008 年复旦计算机与信息技术系信息安全本科毕业。2011 与 2013 年分别获得加拿大西门菲莎大学计算科学硕士，统计学硕士学位。2017 年多伦多大学统计博士毕业，主攻函数型数据分析和微分几何统计。研究兴趣包括非欧几何统计，统计机器学习，及分布式机器学习在区块链中的植入。

史逊博士　区块链顾问

在美国硅谷就职于视频处理上市科技公司 Harmonic Inc.，2012 年获得多伦多 York 大学博士学位，主攻计算机视觉识别 computer vision 和人工智能，2006 年北航计算机系研究生毕业。目前担任视频压缩算法设计工程师。他主攻计算机软硬件算法的理论及工业化研究，特别是对区块链，密码学，加密网络，去中心化视频直播有独特的见解。

Louis Cleroux　区块链专家

Louis 与早期阶段的企业家合作，希望改进/重构以太坊和比特币等区块链技术。他最新的技术投资项目围绕智能钱包和智能应用程序。

关宇　区块链顾问

. NET / C# / Azure Cloud / DevOps/ 微软技术专家，高级架构师。从事软件架构，设计，研发工作将近二十年。早年就职于微软亚洲工程院。曾成功带领团队针对北美客户实施中大型软件研发交付。现经营一家科技驱动型北美地产管理公司，时任公司 CTO。获得微软 CEO Satya Nadella 亲自颁发的微软最具价值专家奖 MVP (Microsoft Most Valuable Professional)。

朱斌　云计算顾问

十五年数据库经验，大数据科学家。曾就职于华为，MindGeek，从零建立起 30 人规模的大数据团队，七年以上大数据研发经验，精通各种 RMDB 与 NoSQL db，每日处理 PT 级数据。多年团队管理经验，擅长团队沟通与协调。

Douglas Leahey 商业发展顾问

环境学博士，蒙特利尔青年就业顾问。提供法律，融资，政府相关创新支持项目顾问服务。协助制定公司战略方向和市场推广销售策略。

Jake Barralet　校企合作项目 Mitac 顾问

伦敦大学 QMW 生物医学材料跨学科研究中心博士，他被授予加拿大骨科诱导生物材料研究委员会主席的职位，并致力于这一主题，并延伸以前的工作，包括生物矿化。与 Nebula AI 合作人工智能在生物医学领域的应用。

10 结语

作为全球首个人工智能区块链系统，Nebula AI 致力于推动人工智能技术发展，构建基于区块链的可靠信任机制，创造社会价值以及服务于全人类。智云链构建了下一代人工智能区块链基础平台，让众多行业开发者无需顾虑底层开发、系统配置以及环境搭建，真正实现高效率，低成本，安全可信的人工智能开发、计算及部署。

智云链可以被认为是一种对去中心化数据的共识系统，NBAI 代币作为价值的载体，实现了人工智能在智云链生态系统的价值流动。传统互联网能够解决数据的通讯问题，而智云链则在传统互联网的基础上更进一步地解决了数据的共识问题。同中心化的大型平台相比，智云链能够避免被服务商保存或窃取数据，真正实现公开处理任务的同时保证数据私有。

区块链技术的迅猛发展，将数字化信用社会的实现变成了可能。智云链将为全球区块链技术的发展注入更多新鲜充满活力的血液，并期待把人工智能这一能够变革人类社会的重要领域推向新的巅峰。

参考文献

[1] Iris Belle. The architecture, engineering and construction industry and blockchain technology.

[2] Juan Benet. Ipfs-content addressed, versioned, p2p file system. *arXiv preprint arXiv:1407.3561*, 2014.

[3] Evangelos Benos, Rod Garratt, and Pedro Gurrola-Perez. The economics of distributed ledger technology for securities settlement. 2017.

[4] Vitalik Buterin et al. A next-generation smart contract and decentralized application platform. *white paper*, 2014.

[5] Matteo Campanelli, Rosario Gennaro, Steven Goldfeder, and Luca Nizzardo. Zero-knowledge contingent payments revisited: Attacks and payments for services. In *Proceedings of the 2017 ACM SIGSAC Conference on Computer and Communications Security*, pages 229–243. ACM, 2017.

[6] Sinclair Davidson, Primavera De Filippi, and Jason Potts. Economics of blockchain. 2016.

[7] Ben Laurie and Richard Clayton. Proof-of-work proves not to work; version 0.2. In *Workshop on Economics and Information, Security*, 2004.

[8] June Ma, Joshua S Gans, and Rabee Tourky. Market structure in bitcoin mining. Technical report, National Bureau of Economic Research, 2018.

[9] marketsandmarkets.com. Blockchain market worth 7,683.7 million usd by 2022. `https://www.marketsandmarkets.com/PressReleases/blockchain-technology.asp/`.

[10] J-P Martin and Lorenzo Alvisi. Fast byzantine consensus. *IEEE Transactions on Dependable and Secure Computing*, 3(3):202–215, 2006.

[11] David C Mills, Kathy Wang, Brendan Malone, Anjana Ravi, Jeffrey C Marquardt, Anton I Badev, Timothy Brezinski, Linda Fahy, Kimberley Liao, Vanessa Kargenian, et al. Distributed ledger technology in payments, clearing, and settlement. 2016.

[12] Armin Nabaei, Melika Hamian, Mohammad Reza Parsaei, Reza Safdari, Taha Samad-Soltani, Houman Zarrabi, and A Ghassemi. Topologies and performance of intelligent algorithms: a comprehensive review. *Artificial Intelligence Review*, 49(1):79–103, 2018.

[13] Satoshi Nakamoto. Bitcoin: A peer-to-peer electronic cash system. 2008.

[14] Nvidia. Geforce gtx 1080 ti. `https://www.nvidia.com/en-us/geforce/products/10series/geforce-gtx-1080-ti/#performance`.

[15] Svein Ølnes. Beyond bitcoin enabling smart government using blockchain technology. In *International Conference on Electronic Government and the Information Systems Perspective*, pages 253–264. Springer, 2016.

[16] OntarioHydro. Electricity rates by province. `http://www.ontario-hydro.com/electricity-rates-by-province`.

[17] Wessel Reijers, Fiachra O'Brolcháin, and Paul Haynes. Governance in blockchain technologies & social contract theories. *Ledger*, 1:134–151, 2016.

[18] Klaus Schwab, Xavier Sala-i Martin, et al. The global competitiveness report 2010-2011. Citeseer, 2010.

[19] Brett Scott. How can cryptocurrency and blockchain technology play a role in building social and solidarity finance? Technical report, UNRISD Working Paper, 2016.

[20] Marten Van Dijk, Craig Gentry, Shai Halevi, and Vinod Vaikuntanathan. Fully homomorphic encryption over the integers. In *Annual International Conference on the Theory and Applications of Cryptographic Techniques*, pages 24–43. Springer, 2010.

[21] MGCSA Walport. Distributed ledger technology: Beyond blockchain. *UK Government Office for Science*, 2016.

[22] Guy Zyskind, Oz Nathan, et al. Decentralizing privacy: Using blockchain to protect personal data. In *Security and Privacy Workshops (SPW), 2015 IEEE*, pages 180–184. IEEE, 2015.

A 修订记录

28/02/2018 私募轮硬顶由 25,000 ETH 调整为 18,000 ETH。
公募轮硬顶由 24,000 ETH 调整为 12,000 ETH。
取消建设 10MW 的人工智能计算中心的计划，
调整为与大规模的第三方互联网数据中心合作，为 AI 计算提供算力。
调整合作伙伴和合作项目。
调整代币分配比重。
新增顾问成员。

07/03/2018 新增研发团队成员。

16/03/2018 调整私募时间。

19/03/2018 调整 ICO 软顶。

09/04/2018 新增研发团队成员。
调整私募剩余代币，与公募合并。