Ulord：基于区块链技术的价值传播网络

技术白皮书

Version 1.2.2

Ulord 基金会
http://ulord.one

5000 年前，人类发明文字，开启知识传递信息的文明之旅；

1000 年前，人类发明印刷术，揭开知识传递力量的重要篇章；

近年，人类发明计算机和互联网，信息高速公路开启；

今天，我们有了 Ulord，让知识价值的公平传递成为现实……

Ulord——开启数字资源付费的新时代！

我们致力于打造一个开放、平等、尊重创造的区块链数字资源分发平台。

目　录

摘　要

随着互联网技术深入发展，网络和服务朝着高度中心化的方向演进，带来网络臃肿、效率低下、代价高昂等问题。区块链技术的出现为互联网世界迎来了新的革命，即用去中心化、可信赖的技术代替传统的中心化角色，将整个世界组织成庞大的价值传播网络，实现了从信息互联网到价值互联网的快速进化。近年来，伴随数字虚拟货币市值不断攀升，区块链技术得到了全世界范围内广泛关注，但大量的投资者们仅仅把数字货币作为增值、保值工具，忽略了区块链真正的价值，如何推动区块链技术发展并且落地应用，成为了互联网世界里一个极大的挑战。

本项目围绕主节点系统、投票机制、星际域名系统、侧链技术、共识机制、智能合约、机器学习算法等区块链、人工智能方向的关键技术进行深入研究，旨在开发一条能够适用于众多应用场景的公链。基于该公链建立一套完整的协议，提供各类友好的 API，允许第三方开发商在其开源协议之上构建自己的应用程序，可以广泛应用于知识经验分享、广告投送、代码分享、直播视频等领域，变革和重塑这些领域的行业现状，让信息资源发布者和消费者之间的中心化平台不再成为资源和价值传递过程的主导者，从而打破互联网难以有效传递价值的桎梏，让知识信息传递和价值传输更加通畅而广泛，逐步建立基础公链、链上应用、价值创造、信息消费、开源社区开发者等众多角色共同参与的良好生态。

1 前言

区块链的诞生，标志着人类开始构建真正可以信任的互联网。区块链本质上是记录了所有交易或者数字事件的分布式数据库，也可以认为是一部公共账簿，可以由所有的参与方访问并且记录。区块链能够在网络中建立点对点之间可靠的信任，使得价值传递过程去除中介的干扰，既公开信息又保护隐私，既共同决策又保护个体权益，内在的机制提高了价值交互的效率并降低了成本，具有广阔的应用前景。这项颠覆性的技术中蕴含着海量机会，由其引发的一场变革才刚拉开序幕。

Ulord 重点打造一条点对点价值传递的公链，允许第三方开发商在其开源协议之上构建自己的应用程序，即基于该公链可以搭建各类场景应用，包括文字、图片、音乐、视频、软件等。第三方开发商可以发行代币，构建自己的经济体系，也可以围绕 Ulord 重点打造各类应用，使用 Ulord 中的 UlordToken 作为系统内凭证。比如，可以在 Ulord 上面搭建经验分享平台，经验分享者给发布的经验进行定价，获取经验信息的人在平台上交易，支付给经验分享者的每笔费用都会即时到账；产品推广者可以在 Ulord 上发布广告，对广告进行定价，对广告感兴趣点击广告的人可以得到一定收益；三维动画的制作方可以在 Ulord 上搭建站点，兜售自己的动漫素材，有需求的人直接对素材进行付费，等等。区别于以往信息传递要借助平台或其他中心化机构才能进行传播获利这一模式，去除中间环节，信息提供者与消费者直接通过 Ulord 平台对接，保证了原创者利益的最大化。

为了支持去中心化价值网络的构建和运营，针对其应用特点，Ulord 平台将底层区块链服务和 P2P 分布式服务完美融合在一起，为广大用户提供优质的、基于区块链的互联网价值传递服务。Ulord 主要由 Ulord 平台和 Ulord 原链两部

分组成，其中 Ulord 平台提供海量的云存储空间、高 QoS（Quality of Service，服务质量）的数据分享服务、便捷的站点部署等，具有良好的用户体验；Ulord 原链引入主节点网络，提供稳定网络和存储基础设施，通过投票和预算机制确保 Ulord 整个生态健康有序的发展，结合智能合约能让用户便捷部署分布式应用，完美地支撑整个生态。

这份白皮书详细介绍了 Ulord 项目的设计理念、功能和创新点、体系结构、关键技术以及应用场景。

2 设计理念与创新点

2.1 背景

科学技术是历史发展的火车头，造就新的社会形态；科学技术的发展推动生产力内部各要素发生变革，引发产业结构的调整、经济形式的变化以及经济增长方式的转变，进而推动社会生产关系发生相应变化。从历史发展进程看，铁制农具的出现让人们耕地的能力和效率大大提高，从而打破奴隶主压迫一大群奴隶集体耕种的局面，出现了以家庭为单元的农耕模式，并且极大的拓展了可以耕种的土地，出现封建社会的生产关系；第一次科技革命开创了以机器代替手工劳动的时代，工业生产需要大规模的协作生产，于是农民从家庭劳作走向工厂上班，形成工业社会的生产关系；到了信息化时代，网络让人与人之间可以没有物理距离的限制，数据成为重要的生产资料，也带来了信息时代新的生产关系，数据即是财富逐渐被人们所普遍接受。但是到了互联网普及的今天，是不是我们每个人拥有的数据都可以变成财富呢？未必如此。我们的大部分数据都没有产生价值，有些数据甚至被某些平台利用起来成为其创造财富的重要资源。这个世界需要改变，我们要把数据创造财富的权利回归到数据创造者手中，就像劳动者要拿回属于自己的耐以生存的土地一样。信息技术突飞猛进的发展必然催生出信息社会新的生产关系。

互联网建立之初，其本质就是倡导的是一种自由平等的思想。但拥有数据与数据变现能力的差距造成了理想与现实的鸿沟。在数据交易和知识传递过程，诸多问题不容忽视：

- **版权确认难，信息创造者难以得到相应回报**

近几年随着版权经济的迅速发展，人们的版权意识逐渐增强，事实上除了传

统的书籍、音乐、电影有版权以外，很多个人创作或经验也有版权，但是这种版权往往难以确认，个人想得到回报的方式往往是靠流量或影响力变相获利，难以让自己的一些创意或经验获得回报。而且即使是有办法确认版权的作品，也是中心化的传播机构或平台起主导作用，尤其是一些行业内已经形成巨头对信息传播起决定性作用，创作者想得到用户认可必须服从中心化机构制定的规则，交易过程繁琐，处处“受制于人”，难以得到合理的权益，这种局面严重挫败了创作者的积极性与创造性。

- **创作质量稂莠不齐，用户难以快速获取优秀作品**

在流量为王的移动互联网时代，大众的注意力成为新的稀缺资源，然而，当大量标题党、哗众取宠的信息涌入信息平台时，用户往往在短时间内面对大量的信息，难以做出有效的甄别，甚至是被大量垃圾信息、广告信息充斥眼球。这一现状导致优质的信息变得“曲高和寡”，其创造者的生存空间遭到严重威胁。自然而然，我们无法苛求创作的高质量生产和高效传播，最终造成“劣币驱逐良币”。如果靠中心化平台方自律来改善现状，无异于痴人说梦。经济基础决定上层建筑，只有颠覆性的技术和机制才能完成这场革命。

- **互联网信息爆炸，信息与用户的精准匹配度不高**

信息平台非常注重如何捕获用户，在广告营销、运营管理、品牌塑造上花费巨大代价，但如何进行进一步的产品升级才能应对竞争日趋激烈的市场投入不够。在用户习惯、兴趣的深度挖掘，信息推送的精准度方面还有很大差距。比如在广告投送上，人们都是被动的接受广告，产品推广方要给广告传媒公司支付大量的费用，却不一定可以精准推送给潜在用户。目前所谓的信息精准投送是从用户行为习惯入手去挖掘潜在客户信息，这种方式对数据拥有的门槛很高，最终往往只

有“寡头数据”平台才有机会通过技术去实现。

面对巨大的市场前景，区块链技术作为一种解决上述问题的有效途径，已引起部分嗅觉灵敏的技术爱好者和投资者关注。目前已经有一些项目，都在尝试着利用区块链做信息和内容行业的变革，但都处于起步阶段，尚无非常出色的产品或模式能够给行业带来颠覆性变革。

2.2 设计灵感

区块链作为新一代互联网的底层协议，在它基础上建立的一切应用，天然拥有一个几乎独立的经济体系，而这个经济体系中的利益分配规则又可以用智能合约进行明确定义。

提出并开发 Ulord 项目，主要出于以下三个方面的考虑：

第一，区块链技术的特点可以有效解决版权行业问题，即将版权确认与分发相统一，变革并重新定义当前广告、文娱、出版行业的发布模式。去中心化之后版权产业只剩下两个最基本的角色：创作者（Producer）和用户（User），在这种情况下，利益将重新进行高效合理的分配。迫切需要解决针对版权行业所面临的技术难点和机制创新。

第二，目前区块链还处于初级发展阶段，出现了很多公链，同时也诞生了各种各样的应用，但能有效支持数字资源传递的公链尚未出现，无法承载各种丰富的网站服务类型，尤其是在数据存储、数据服务质量、内容付费模式等方面存在诸多问题，需要专门设计解决知识传递痛点的区块链平台。

第三，从区块链技术本身来看，现有的区块链技术还有许多亟需解决的问题和瓶颈，如网络拥堵、支付时延长、挖矿中心化趋势明显、资源消耗高、部分公

链存在安全漏洞等，难以满足现实应用需求，迫切需要针对上述问题深入开展区块链底层技术研究与实践，推动区块链技术的快速应用和发展。

Ulord 是一个基于区块链技术构建的分布式 P2P 网络开源项目。不同于我们日常所访问的 Internet，在 Ulord 中没有服务器的概念，所有网络数据都被分散在各个 Ulord 用户的电脑中，任何人都只需要一对非对称密钥，就能发布自己的站点。所有人都可以通过搜索、域名等发现发布者公布的站点服务，在 P2P 网络中找直接下载站点的数据。越来越多人访问后，发布者的站点就会被多台电脑保存，那些访问过你的网站的电脑就会开始为你的站点做种子，就像我们所熟知的 BT 种子一样，你的站点的内容就这样在无数台电脑中存续。在 Ulord 网络中，为了提供更好的用户体验，采用两种角色节点存储数据，一种是主节点角色，这种角色的用户通过提供高 QoS 保证的存储服务，用于存储 Ulord 网络上的数据，同时按提供的存储空间赚取收益；另一种是普通用户电脑角色，该角色只会备份用户喜欢的资源，作为主节点角色的补充。用户访问站点服务时，通过分布式哈希表（DHT，Distributed Hash Table）技术让用户快速地从 P2P 网络中下载需要访问的数据片段，然后由客户端组装，恢复出完整的数据。由于采用 P2P 技术承载，Ulord 上的资源具有高可用、永不宕机的特征。

2.3 创新点

从设计上，我们会把这个系统隔离为两个层面，底层的“操作系统”和上层的“应用程序”。透明公开不可篡改的账簿、智能合约的基础架构等建立在底层，而上层的应用程序则用来完成业务逻辑和不需要考虑去中心化应用如何开发。

就支撑数据信息发布平台的原链而言，我们将基于这一应用场景开展一些原创性的工作，包括：

- **引入主节点系统，解决通信延迟大、存储空间小等问题**

设计了新的 POS 机制（Proof of Storage, PoS），鼓励用户和投资者参与主节点网络建设，提供稳定的 QoS 数据存储服务；提供多种跨平台的解决方案，方便用户部署主节点服务，包括 Linux/Windows/OS X 等主流操作系统；通过主节点服务，可支持每秒 4000 笔以上的交易频次，更好地满足现实应用。

- **建立投票机制，促进社区发展并进行内容审查**

允许 Ulord 上的每个用户能对 Ulord 网络上的资源、站点及改进建议进行投票，达到两个目的：一是对开发者提出的预案进行评估，推进社区对 Ulord 的贡献；二是对 Ulord 上的资源和站点进行审查，维护 Ulord 生态健康有序发展。

- **设置合理的收益分配机制，激励广大开发者贡献力量**

留出 10%的收益给整个社区的开发者，资助开发者执行有意义的开发计划。引入代码审查和任务质量评估机制，监督资助的项目按时按质完成，最终形成良性循环，促进 Ulord 生态健康发展。

- **建立星际域名系统，提供唯一的、精简可读的域名服务**

对于区块链上的资源，通常需要用 34 个字符串长度的地址来表示，不容易被用户记住，现实中使用不方便。在 Ulord 设计中，通过建立星际域名系统（InterPlanetary Domain System, IPDS），为用户提供去中心化的域名解析服务。

- **引入侧链技术，实现智能合约的快速部署**

通过侧链技术，能很好地兼容以太虚拟机，发布智能合约。任何用户通过友好的 API 在 Ulord 上搭建站点，提供互联网信息分发服务，且能够自定义自己的代币，通过代币运营自己站点。代币可以以一定比例与 UToken 进行兑换。

- **采用 PoW 和 PoS 混合的共识机制，吸引更多闲置资源加入 Ulord 网络**

为了更好地承载 Ulord 平台上应用，设计实现了一种混合共识机制：PoW（Proof of Work）和 PoS（Proof of Storage）。PoW 算法的作用是用于记账，采用了一种 CPU 挖矿算法 CryptoNight，其通过使用 AES 算法及改进算法，可以有效抵抗各种已知攻击和未知攻击；PoS 算法适用于构建 IPFS 基础设施，鼓励更多的用户提供大的存储空间用于存储 Ulord 上的平台数据。

Ulord 平台层和应用层的主要创新点包括：

- **设计并实现了基于区块链的分布式文件存储、检索和分发机制**

基于底层区块链集成 P2P 下载、分布式文件组织、智能学习等功能模块，提供快速内容搜索服务、分布式存储服务、节点定制化服务、点对点数据分发服务、分布式哈希索引服务、网络资源自净化服务等。

- **设计并实现了一种高效的价值传播模型**

建立分发过程的价值传播网络，通过收益分配机制鼓励用户积极参与，形成用户愿意贡献有价值内容并高效完成优秀内容传播的良好生态。

- **基于人工智能算法支持智能推送**

a）针对特征数据维度高、类型混杂、时效性强等特点，设计了一种基于深度神经网络的多源知识抽取和关联方法，实现针对站点、内容、作者等要素信息的实体名称识别、实体属性抽取等功能；

b）通过混合模型方法、基于知识嵌入的协同推荐方法以及基于在线实时反馈的推荐方法等，实现对不同用户不同维度的内容智能推荐；

c）基于领域知识的混合推荐方法，通过内容向量空间建模技术综合知识结构特征、主题特征、语义特征等，实现基于内容的推荐方法与协同推荐方法的混

合推荐。

- **基于人工智能算法进行内容控制与促进传播**

a）通过向量空间建模技术综合知识结构特征、主题特征、语义特征等，对敏感信息进行自动审查；

b）基于知识图谱进行传播路径选择和优化，通过关联内容的组合提升内容访问量，提升用户体验。

这些技术路线和生态体系的创新设计，为 Ulord 提供有力的支撑，并试图对目前信息资源分发行业的现状进行革新，推动其健康发展。

2.4 发展愿景

Ulord 旨在通过去中心化的方法重构信息传递的利益分配。让所有的数据和知识都有价值，让所有的价值都回归到创作者手中。让信息的自治权和收益权由信息生产者决定，减少中间环节对信息的控制和价值折算。

Ulord 是通过区块链技术改造互联网世界的利剑。

- **新体系下的知识付费——价值有效传递**

在去中心化的体系中，知识只有收费和付费两种，前者是想看就要付钱的，如小说、音乐、影视，后者是付费求别人看的，如广告。不管是收费和付费，信息发布者直接将价值进行有效传递，不需要中间环节进行议价或消耗资源。传统的中心化平台失去议价权，是不是就没有动力参与到新的体系内呢？仍然有更大的动力加入。对于很多知名度不高的创作者，会跟平台方合作，主动让出一部分利益已快速让作品进入市场，对于优秀的内容，作者和平台方可以从中获得更大的价值。

- **新体系下的用户行为——创新发行机制**

用户对知识或信息的处理，有阻止传播和促进传播两类，如发表差评表示阻止传播，发表好评表示促进传播，如转发就是新的信息发行机制。去中心化的网络可以使用共识机制为产生行为的用户打分，从而找到真正有能力鉴别和孵化内容的用户。一旦用户进行转发，用户就相当于发挥了分发能力，理应收到知识或信息带来的回报，转发的轮次越多，回报也相应更多。事实上，通过合约机制，用户在完成知识或信息转发的过程，就是向原作者购买版权的过程（原作者不断得到收益）。

- **互联网的价值革命——优币淘汰劣币**

对稂莠不齐的信息说“不”，通过技术和机制进行价值的筛选，有价值的信息可以脱颖而出，无价值的信息被机制淘汰。比如，对于出版行业而言，制作、发行、分发的后两个动作（发行与分发）全部由用户完成，而新的利益分配方式也使得他们有足够的动机做得更好。于是，内容制作将更为精良，优秀的创作者更为心无旁骛——因为只要确保做出世界真正需要的东西，根本就不用害怕“怀才不遇”。我们立志于依托于区块链技术建立一种互联网新秩序。

- **去中心化的新世界——生态圈与孵化器**

没有任何应用可以“满足所有需求”，所以在 Ulord 上可以开发多种应用，它更像是一个区块链应用孵化器。在此基础上，我们会开发和投资多个具体应用。第一个 Ulord 的应用将由我们自己开发作为示例，它是一个基于强关系的信息发布系统，在此基础上添加了智能合约，以进行利益的重新分配，真正让数字内容的生产者和分发者得到回报。不断降低传统平台接入区块链的门槛，用户并不需要深入了解链上技术，通过调用友好的 API 即可发布自己的应用。

总之，Ulord 立志于运用区块链技术打造新一代的数字信息交互平台，定位

于打造一条基础公链。遵从自由、开放、尊重创造的思想，面向全球的生态系统，具有版权确认与分发、无平台费、集成支付系统、支持不同数字内容格式、交易更便捷等优势。

3 Ulord 的体系结构

Ulord 在整体设计上采用松耦合的模块化设计方式，鼓励更多的开发者加入整个生态的开发。通过 web 界面、桌面应用及移动 APP 等多种展现形态让应用层发布者能更便捷的搭建站点，发布属于自己的互联网信息分发服务。Ulord 的体系结构如图 2 所示，由 Ulord 平台和 Ulord 原链组成，其中 Ulord 平台是 P2P 数据服务，包括数据传输、数据分发、数据存储、数据索引、计费模型、传播模型、Gas 模型及支付系统等等，Ulord 原链为区块链基础设施，为 Ulord 平台提供记账、域名及主节点等服务，确保整个骨干网络稳定有序。

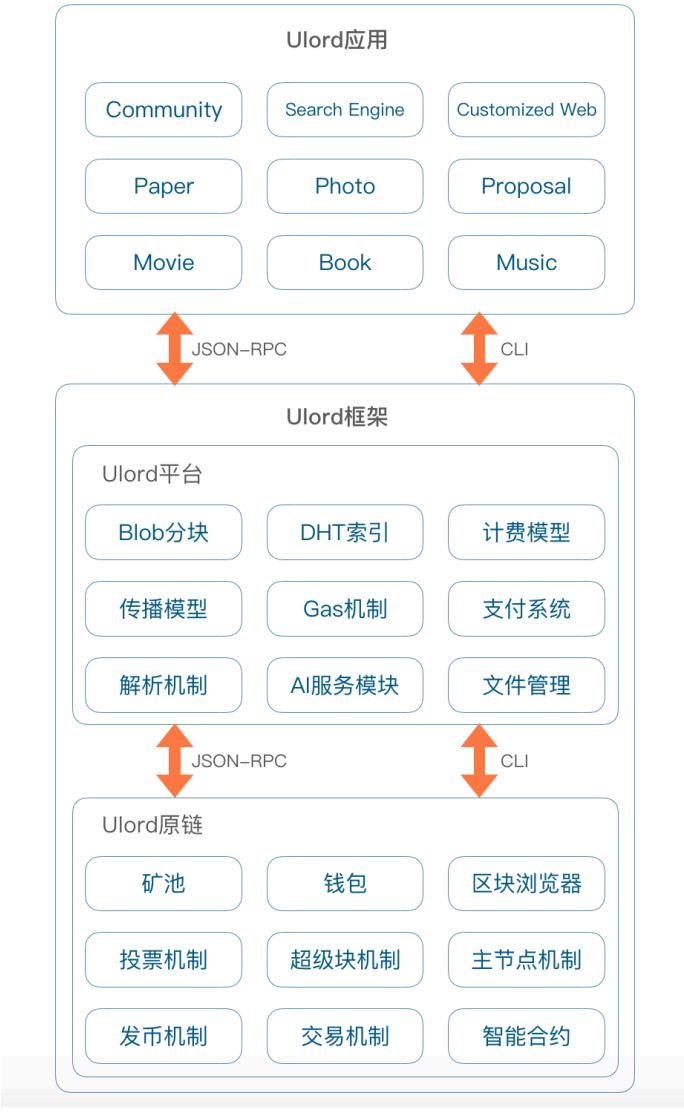

图 2 Ulord 体系结构

4 Ulord 平台

平台层为系统中间层，在应用层和基础层之间起着桥梁作用，平台层根据组件功能分类支撑组件和功能组件两部分。支撑组件为功能组件提供基础功能支撑，平台层通过功能组件连接基础层区块链，从而为应用层提供基于区块链的信息分发、共享及支付服务。平台层架构图如图 3 所示。

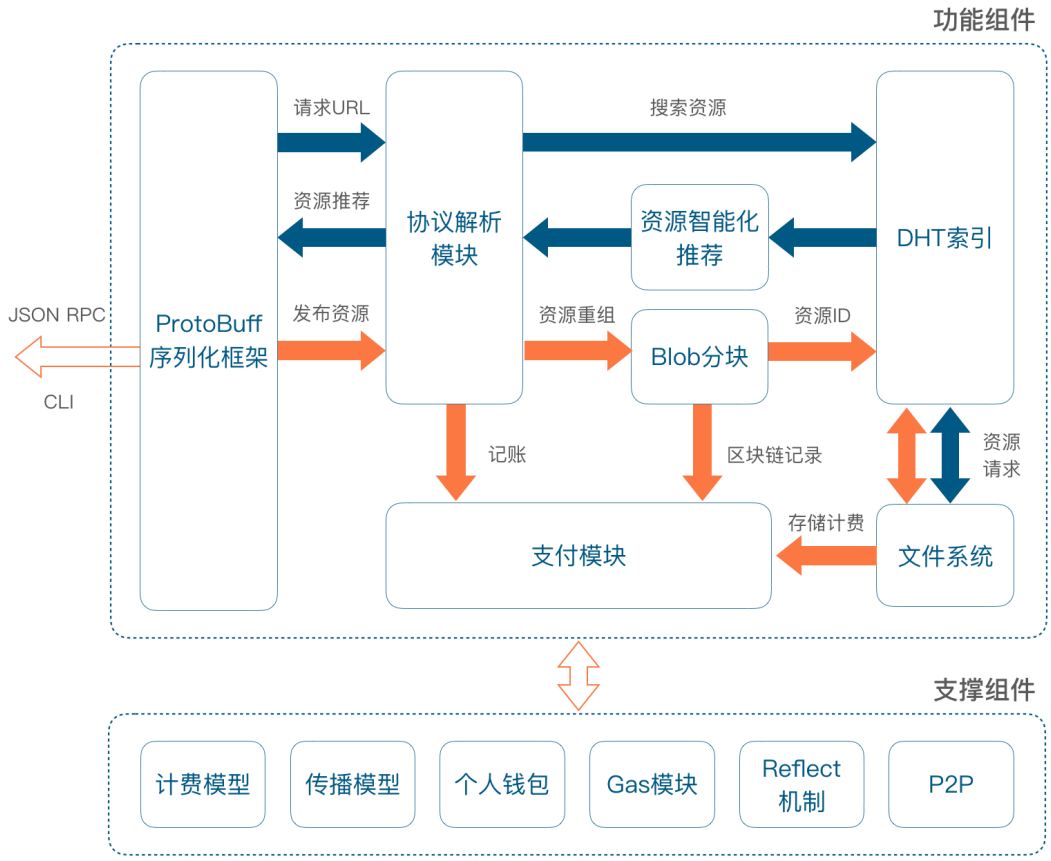

图 3 平台层架构图

平台层的核心功能在于为信息分享平台构建一个内容共享的基础网络环境和服务环境，主要功能模块如下。

4.1 Ulord 协议

Ulord 协议是数据传输及服务层的基础，用户基于 Ulord 协议可以快速上传

资源、搜索并购买感兴趣内容。Ulord 协议通过定义一系列的规则实现数据的分布式组织及计费。

- 分布式总账

Ulord 协议的基础是分布式总账，它是生成加密货币（UlordToken）的基础。Ulord 系统与传统银行和支付系统的不同之处在于它是去中心化的信任系统，这种信任机制是通过不同参与者的相互作用而达成的。系统执行交易时，通过分布式共识机制变得可信，被接受的每一笔交易都会记录在区块链中，即建立分布式账簿。

Ulord 内部数据存储采用键值对的方式，每个键对应为相应资源或者其元数据的名称，通过基于键名称的搜索返回用户关注的内容资源。Ulord 区块链上除存储资源的名称、支付信息等元数据外，其余数据存储方式与比特币区块结构保持一致，但是本项目对区块 hash 算法、区块奖励函数、区块大小、总区块数以及支付系统等进行了优化。

- Ulord 网络

Ulord 网络是扩展 Ulord 区块链原有记账、支付功能的基础设施，其主要功能是为用户在区块链中进行支付、搜索、下载、上传资源提供网络环境。接入 Ulord 网络是进行内容分发共享的前提条件，与传统 www 互联网所使用的 HTTP、DNS 或者其他协议功能类型不同，Ulord 网络基于 Ulord 协议进行用户通信及数据交换，在应用形式上 Ulord 网络表现为后台运行的守护进程，一方面监听本机的数据请求，另一方面监听网络中的其他节点，与之进行数据交换。

4.2 Ulord 网络服务

Ulord 服务以 Ulord 协议为基础，集成 P2P 下载、分布式文件组织、智能学

习等技术组成不同的功能模块，Ulord 网络服务可以根据用户需求进行灵活设置。目前提供的服务主要包括以下几类：

- 快速内容搜索服务

Ulord 协议提供了基于元数据的资源分类功能，每个用户资源除了可以按照传统的基于描述信息的搜索功能外，还具有以下特性：

✓ 提供基于内容寻址的资源快速定位，而非基于域名寻址。文件具有存在的唯一性，即一个文件加入到 Ulord 网络，将基于计算对内容赋予一个唯一加密的哈希值。

✓ Ulord 网络上运行的区块链除了存储交易 hash 值外，对其进行了扩展，支持用来存储文件的哈希值表，每次有网络访问，即要在链上查询该文件的地址。

- 分布式存储服务

Ulord 使用 P2P 的超媒体协议，可以让网络更快、更安全、更开放。Ulord 网络中的所有节点构成一个面向全球的、点对点的分布式文件系统，将所有具有相同文件系统的计算设备连接在一起。每个文件及其中的所有分块都被赋予一个称为加密散列的唯一指纹。每个节点通过判断文件的哈希值判断哪些冗余重复的文件，在单个节点上确保数据不冗余。查找文件时，通过文件的哈希值就可以在网络中查找到储存该文件的节点，找到想要的文件；Ulord 下一步计划提供文件的历史版本控制器，支持多节点使用并保存不同版本的文件，实现文件历史状态跟踪。

其次，Ulord 中文件存储不强制要求每一个节点都存储所有的内容，节点的所有者可以自由选择想要存储的数据，对于存储大量内容信息的节点，Ulord 计

费模型通过文件下载服务的数据量自动计算用户收益，以此激励用户升级其硬件资源以提供更全面的数据存储和维护服务来获取收益。

- 节点定制化服务

Ulord 网络节点包括中心化节点及轻量化节点两大类。中心化节点具有存储 UlordToken 交易全部历史记录（每个用户每次交易）的客户端，管理用户钱包，并且可以直接在 Ulord 网络上启动交易。这种节点能处理协议的所有方面，并可以独立验证整个区块链和任何交易，可以提供完全自主和独立的交易验证，但中心化节点客户端需要消耗很多计算机资源（例如，超过 125GB 磁盘，2GB RAM）。轻量化节点部署轻量级客户端，一个轻量级客户端，也称为简单支付验证（SPV）客户端，连接到 Ulord 完整节点，用于访问 Ulord 交易信息，但是在本地存储用户钱包，并独立地创建、验证和传输交易。轻量级客户端与 Ulord 网络直接交互，无需中介。

- BitTorrent 点对点内容分发服务

Ulord 在区块链记账的基础上集成了 BitTorrent 点对点数据分发协议，采用高效的软件分发系统和点对点技术共享大体积文件（如一部电影或电视节目），并使每个用户像网络重新分配结点那样提供上传服务。传统网络中，下载服务器为每一个发出下载请求的用户提供下载服务，而 BitTorrent 的工作方式与之不同，分配器或文件的持有者将文件发送给其中一名用户，再由这名用户转发给其他用户，用户之间相互转发自己所拥有的文件部分，直到每个用户的下载都全部完成。这种方法可以使下载服务器同时处理多个大体积文件的下载请求，而无须占用大量带宽。

- 分布式哈希索引服务

Ulord 网络使用了分布式哈希表（DHT，Distributed Hash Table）来组织用户资源的命名空间，通过 DHT 在网络节点中实现（key，value）的关系映射。DHT 是一个不存在中心点的、提供 key->value 查询功能的分布式系统，关于 key 到 value 的映射信息分布式地保存在多个节点上，数据的变化和节点的变化只会影响到部分节点，不会对所有节点产生影响。作为一种基础架构，DHT 可以用来构建更多复杂应用，比如分布式文件系统、域名服务、即时消息、P2P 文件共享和内容分发平台。DHT 定义一个关键字空间，比如所有 160 位的位串集合，然后通过某种算法，把这些关键字映射到整个 DHT 系统的所有节点上。这种算法称为一致性哈希（consistent hashing）。通过这种算法，DHT 可以根据某个关键字找到某个节点，然后对该节点进行操作，比如存数据、查数据等。

DHT 中的每个节点只需要与其他部分节点相连即可，使用某个关键字访问任何一个节点，这个节点都可以将信息前传到该 key 对应的节点上进行处理，这种处理叫做基于关键字的路由（key-based routing）。搜索引擎可以通过特征串从 DHT 网络节点处得到种子文件，而不需要依赖种子服务器，BT 下载就借助公有 DHT 网络，可以很大程度上减少对种子服务器的依赖。

- 网络资源自净化服务

Ulord 是一个去中心化的网络，没有中心管理员对内容进行审查和控制，因此不可避免会出现“不当”内容资源，Ulord 设计了网络投票模式，支持用户节点发起提案，对网络中的内容资源进行投票，当投票结果满足一定条件，则识别为“不当”内容，系统中可通过无限提高资源的花费或者将资源离线化，使得“不当”资源不可访问。

- 计费服务

在 Ulord 网络中，资源传播、存储、发布下载等动作除了完成相应应用功能外，都被视为一笔交易存入区块链中。网络中多数交易包含交易费（矿工费），比如发布资源、下载资源等，Ulord 网络中鼓励用户发布、传播高质量的资源，主要的计费行为包括以下几类：

✓ 发布资源，用户对资源进行命名时需存入一笔 UlordToken，存入的 UlordToken 在用户账户中被锁定，不可交易，待资源撤回时，这笔 UlordToken 会在扣除交易费后返还至用户账户；其次用户为用户资源命名时如果网络中已有相同名称，则支持用户提高报价获得优质名称的使用权。

✓ 下载资源：用户在线浏览、下载资源时，按照资源设定的币值支付相应的 UlordToken。

✓ 传播资源：用户分享其他用户发布的资源，当该资源有消费行为时，可从中获取资源传播收益。

✓ 提供存储资源获取收益：用户升级硬件设备，作为中心节点提供存储及下载服务，可获取收益。

✓ 提供计算资源获取收益：用户节点作为矿工的角色参与分布式记账，从中可获取收益。

✓ 发起提案：用户针对网络内容审查发起提案，需支付 UlordToken；

✓ 系统研发/维护：系统会预留一定比例的 UlordToken 用于提案投票、功能研发。

- 综合服务流程

平台层服务主要流程如下：

✓ 用户加入 Ulord 网络，用户通过客户端在网络中搜索叫“XX 喜剧电

影”的文件；

✓ Ulord 网络迅速索引区块链上的哈希值，返回相关搜索结果；

✓ 用户根据返回文件的付费信息支付相应的 UlordToken，将“XX 喜剧电影”文件缓存到本地，此时，“XX 喜剧电影”文件不是从云或者服务器上下载下来的，而是 Ulord 网络中的某个或者某几个最近的网络节点；

✓ 在 Ulord 网络中，用户资源一般都是分块加密后存储于网络节点中，并且每个分块都存储于多个用户节点或者中心节点中，Ulord 网络自动搜索最快的下载方式，将资源进行重新组合，确保用户以最具效率的方式下载到该文件；

✓ 用户将文件缓存在自己电脑以后，不仅可以自己观看，同时也可以为其他人提供资源共享；

✓ 自己也可以在网络上转发该资源，并且有机会获得 UlordToken。

4.3 AI 服务模块

在平台层我们加入 AI 层，AI 层需要处理的数据可以来自两个方面：

（1）应用层产生的运营数据，包括用户行为数据和应用行为数据等。

（2）平台层和基础层的运行数据，通过 AI 技术使得底层系统的运行更加安全、稳定、高效。

AI 支撑的功能主要包括生成管理、质量控制和分发效果管理三个部分。

（1）生成管理

包括热门站点、热门内容实时跟踪；内容实时性、权威性、影响力、吸引力的快速分析；优质作者的信息管理和行为分析，通过各种途径吸引优质内容创作者来建设站点。

（2）质量控制

原创内容审定：配合基础层的区块记录信息，对文章的原创性进行分析，防范恶意模仿、老话新谈。

敏感信息审查：除了投票审查机制外，系统基于 AI 进行低俗内容识别，通过语义分析和图像检测识别、控制涉黄涉政敏感话题。

（3）分发效果管理

精准推荐投送：通过用户访问行为（浏览页、浏览顺序、停留时间）的关注点与兴趣点挖掘，实现对站点内容的个性化精确推送。

传播路径优化：基于知识图谱进行传播路径选择和优化，通过关联内容的组合提升内容访问量，提升用户体验。

恶意节点分析：对内容传播链路中“撸羊毛”的恶意节点进行识别和剔除，保障真实用户的合法权益。

5 Ulord 原链

为了满足互联网数据分发的需求，Ulord 的原链引入了主节点系统，将整个主节点网络构造为点对点的分布式文件分发网络（InterPlanetary File System，IPFS），提供了海量云存储资源池和全球统一的可寻址空间存储资源。考虑 Ulord 的可持续发展，引入了投票系统和预算系统，投票系统不仅能对应用层的多种应用进行智能评判，也能辅助预算系统，资助更多的开发者投入 Ulord 开发，让整个 Ulord 生态发展处在一个良性循环，承载更多的应用。在其他实现上，Ulord 网络能和智能合约兼容，能让以太上的应用移植到 Ulord 网络上。Ulord 采用工作量证明和存储量证明混合挖矿机制，确保区块网络的发展不被算力劫持。

5.1 主节点系统

全节点是指在 P2P 网络上运行完整客户端的服务器或普通 PC 机，在区块链网络中起着传播交易和区块的作用。维持全节点的正常运行，需要消耗大量的网络资源，如存储空间和网络流量等。据 ZapChainMagazine 统计，比特币网络上的全节点数目呈现出逐渐下降的趋势，使区块广播的时间需额外增加 40 秒。社区提出了许多解决方案，如引入微软研究的新奖励计划和 Bitnodes 激励计划等等，尝试着增加节点数目，但都没有得到好的解决。

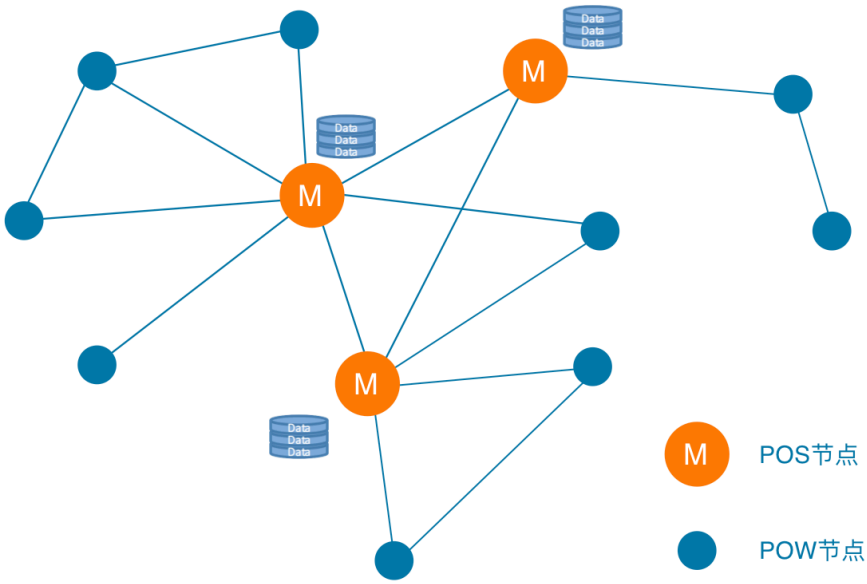

图 4 主节点网络

为了维持区块链骨干网络的健康稳定，达世提出分级网络的解决方案，通过引入主节点系统，组成稳定的骨干网络，解决通信延迟大的问题。在达世的系统里面，存入 1000 dash 的节点即可升级为主节点，若能在一段时间内稳定在线，将分取每个区块网络 45%的收益。但目前来看，达世的主节点系统在设计和实现上仍然存在很多不足。首先，根据达世的设计规则，全系统发币总量大概为 1700 万个，目前已经发行的达世币数目大约为 800 万个，而主节点的数目大概维持在 4800 个左右，由于每个主节点都需要有 1000 个 dash 作为担保，由此推断大约接近 500 万个达世锁死在主节点上，市面上流通的达世数目不足 300 万个，这显然和比特币最初的设计理论相违背，无法保证市场上有足够的币流通。其次，在设计主节点时候，没有做任何的甄别，没有充分考虑 QoS，主节点的服务质量也是参差不齐，导致网络通信没有达到预期效果。最后，只有具备一定的计算机知识才有可能搭建主节点，并不是所有的人具备这样的基础，委托第三

方来搭建主节点往往会带来资产上的风险，让更多的人参与主节点网络的维护很有必要。如图 4 所示，Ulord 考虑不同的应用场景，对主节点系统做了进一步优化和改进，具体如下：

引入主节点候选机制，增强网路服务质量。Ulord 为了鼓励用户加入主节点建设，将整个网络 25%的收益分给主节点持有者。同时引入 QoS 考核机制，采用优胜劣汰的原则，淘汰一些不满足要求的主节点，确保主节点用户必须持续投入和维护才能保证节点的状态完好。QoS 考核机制主要从以下几个方面考虑：

数据丢包率：通过 ping–pong 操作判断主节点与相邻节点的丢包率，超过一定阈值判定节点状态不符合服务要求，淘汰出主节点列表。

网络通信延迟：通过 ping–pong 操作判断主节点与相邻节点的延迟，超出一定阈值判定节点状态不符合服务要求，淘汰出主节点列表。

数据重传次数：当主节点与相邻的用户节点出现重传次数过高时，用户节点会广播全网络，当举报该主节点次数达到阈值时，淘汰出主节点列表。

引入 Proof–of–Storage 机制，提供 IPFS 服务。为了满足 Ulord 的互联网内容分发机制，需要搭建大量节点承载互联网数据，提供更优质的视频流和数据流服务。在 Ulord 网络中，将从两个层面来保证高质量的网络存储服务。首先，在 Ulord 网络中，要成主节点需要提供 1TB 的硬盘存储空间作为资质担保，Ulord 可以通过分布式技术将这些主节点组成一个海量的存储资源池。其次，为了确认每个主节点确实存储了数据，引入 Proof–of–Storage 机制。该机制通过数据持有性证明和数据可恢复证明，随机的对主节点的数据进行完整性验证，确保主节点能稳定提供数据存储服务。主节点考虑因素有：

- 存储容量：根据存储容量大小，按比例计算收益；

- 存储价值：根据存储数据价值，判断是否存储平台有效数据，判断是否计算收益；
- 存储 IOPS：IOPS(Input/Output Operations Per Second)，即每秒进行读写（I/O）操作的次数，衡量磁盘随机访问的性能。根据磁盘性能，判断是否计算收益。

更通用的主节点平台。Ulord 将为主节点用户提供更好的用户体验，同时也为系统自身带来更优质存储和网络服务器。为了吸引更多的投资者参与主节点网络的建设，我们将开发跨平台的主节点客户端软件，包括 windows/Linux/OS x/Android 等多个主流系统。针对 Linux 系统，将直接提供 Docker 封装镜像，便于用户安装。

5.2 投票系统

投票系统在 Ulord 上主要有两个作用，一是对开发者提出的预案进行评估，促进社区对 Ulord 的贡献；二是对 Ulord 上的资源和站点进行审查，维护 Ulord 生态健康有序发展。如果有开发者为 Ulord 贡献好的解决方案或代码，可以得到系统的奖励，判断是否对开发者的贡献进行奖励，或者奖励多少，由社区投票决定。另外，Ulord 允许用户发布属于自己的站点，但有可能带来的问题是大量的应用发布会让整个生态变得无序，难以治理。为了净化网络环境，让 Ulord 生态健康发展，引入共识评判机制，对 Ulord 网络进行智能维护。用户在 Ulord 上发布的资源，都有唯一的 160bit 的 hash 值，所有主节点都可以对 Ulord 上用户发布的站点资源进行投票表决，表明自己的立场。当一定时间内反对的票数超过某一阈值时，网络将会自动禁止资源的传播，并给出时间让发布者整改，若规定时间内，资源没有整改，网络将自动删除。投票类型有 yes、no 和 abstain 三种。

5.3 预算系统

为了促进 Ulord 生态的健康发展，Ulord 预留了 10%的收益给整个社区的开发者。Ulord 给开发社区提供统一提案入口，社区的开发者可以通过该入口提交对 Ulord 的改进提案，提交后的提案会广播到全网络，并以消息的形式推送给用户，Ulord 上的所有用户都拥有投票权，当一个提案支持的数目超过一定阈值时(当前系统设定为 30%)，提案将获得通过。之后，提交提案的开发者将开始接受预算系统支持。同一个提案，用户需要进行两次表决，第一次表决后，开发团队将接受预算的支持，但只会给予开发者 50%的预算，直到开发者完成开发后发起第二次表决，用户才有可能收到剩下 50%的预算支持。

在具体实现上，每隔 17000 个区块，就会自动生成一个超级块，通过该块资助社区的开发者。超级块的 coinbase 币的数目是前一超级块和当前超级块之间的区块扣去 10%收益后的总和，然后 txout 是通过预案的预算地址。若当前超级块没有预案，资金会自动存储到资金池中，用于后续预案预算支持。

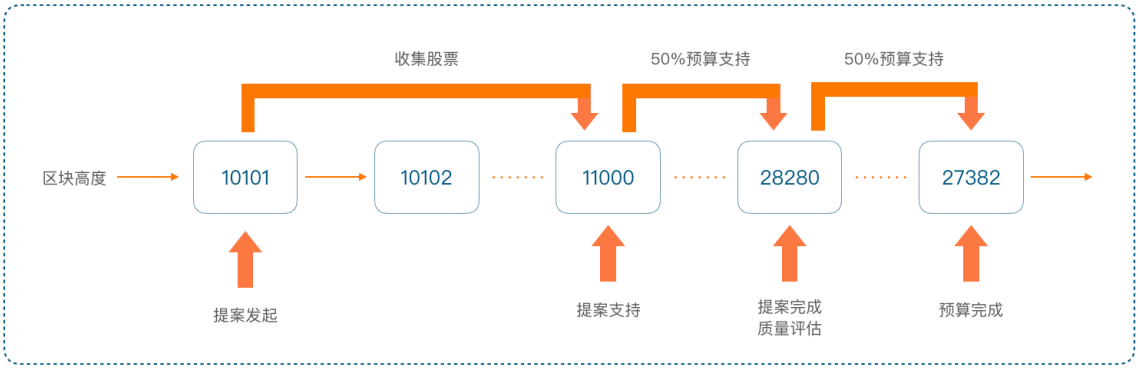

图 5 预算处理流程

5.4 智能合约

5.4.1 统一域名机制

Ulord 允许用户调用平台层的 API，发布自己的站点服务。为了让 Ulord 用户能便捷地访问其他用户在 Ulord 平台上的资源，可以用可读的、易记字符串作为域名。用户发布资源之前，通过指定域名站点可以申请可读、易记的域名，但需要绑定一定的币量，随着时间推移，币量会随着区块的增加而逐渐消耗，换句话说，Ulord 上所有承载的资源、站点都会随着区块高度增加而消耗。用户可以通过充值的方式让申请的域名持续有效。所有因申请域名而消耗掉的币将流入底层网络，变为记账的一部分费用。

为了支持可读域名机制，我们引入一个新的数据结构 DomainClaimtrie，保存 Ulord 上所有的域名及其关联的相关信息。如图 6 所示，在 DomainClaimtrie 里，每个节点对应着一个域名，同时每个节点还保存着该节点相关的交易信息，包括一个交易，用户申请域名时，必须绑定一定数目的币，才允许新的域名注册，域名在 Ulord 网络中是唯一的。支持用户注销域名，注销后，域名自动释放。为了支持域名树的完整性，我们对区块链的区块结构进行了修改，添加了一个字段 DomainClaimtrie。

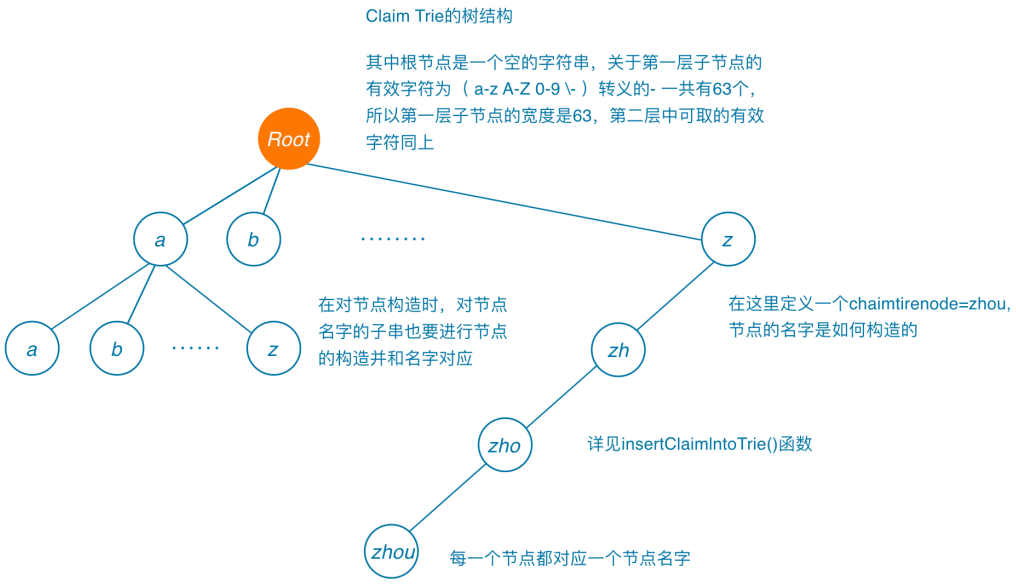

图 6 DomainClaimtrie 数据结构

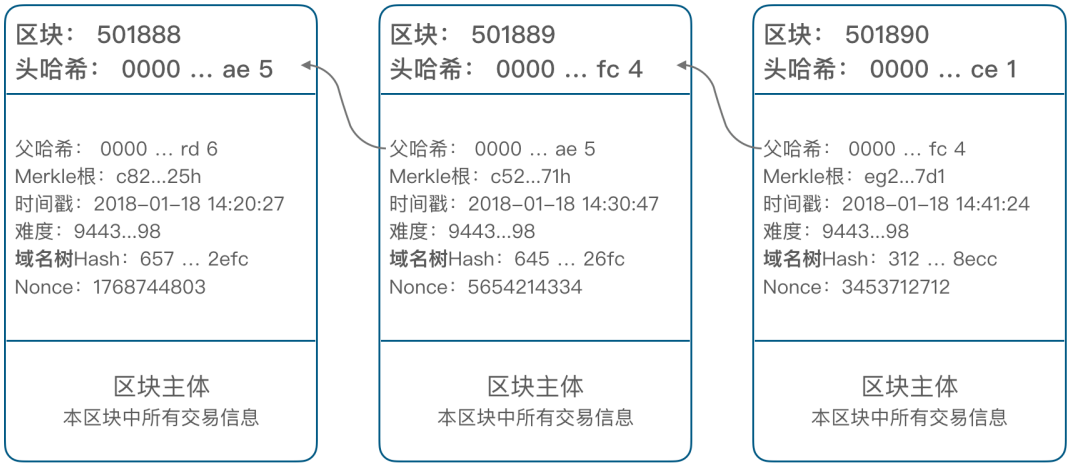

图 7 区块结构

5.4.2 智能合约属性

Ulord 具有智能合约属性，引入了 gas 的设计理念，但不同于以太 gas 每一个操作都会消耗 gas。相比以太的 gas 概念，Ulord 中采用了更简化抽象的方法。用户发布在 Ulord 上的资源和站点都是消耗 Ulord 网络上资源，因此用户发布资源或者站点时候，需要绑定一定量 UlordToken。随着区块高度的增长，UlordToken 会逐渐地消耗掉，用户需要在消耗掉之前往站点对应的地址充入新的 UlordToken，才能确保拥有该域名的所有权。同时通过侧链技术，可以兼容以太虚拟机，发布智能合约，允许用户发布自己的代币，代币与 UlordToken 存在一定比例的兑换关系。Ulord 允许用户自定义的发布自己站点服务，而通过发行自己的代币，可以运营自己的站点。

5.5 共识算法

Ulord 采用 PoW(Proof of Work)和 PoS(Proof of Stake)相结合的方式作为共识算法。其中，PoW 采用 CPU 挖矿算法，通过采用多级串行密码学原语操作，同时结合计算机体系结构特征，具备永久防 ASIC 的挖矿特征。POS 机制主要是

为了鼓励更多的主节点加入，通过提供更多的存储空间，在为自身带来收益同时，也为 Ulord 提供海量的分布式存储空间。

5.5.1 POW 实现机制

为了充分利用闲置的资源进行挖矿，Ulord 原链采用 CPU 挖矿算法——CryptoNight。该算法在随机寓言模型下，被证明是安全的。CryptoNight 算法结构如图 8 所示：

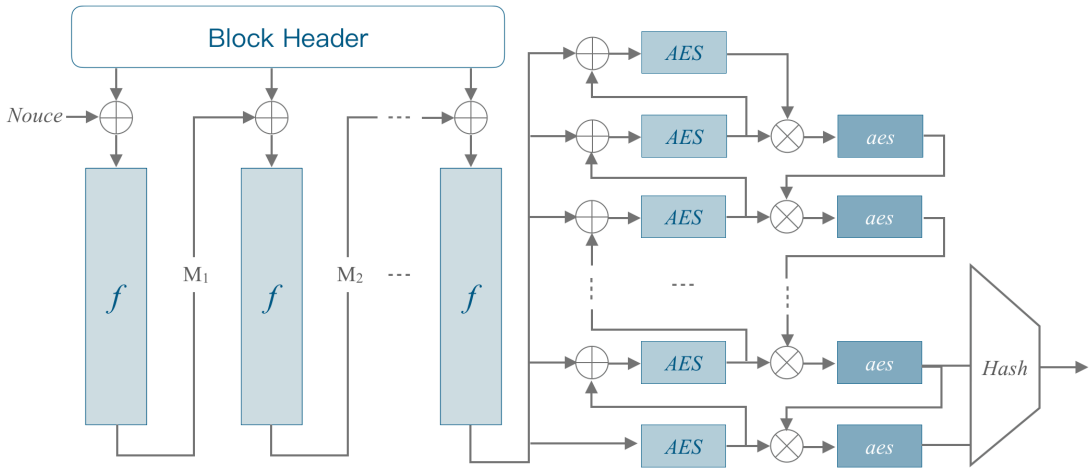

图 8 CryptoNight 算法结构

算法的输入为上一个数据块的 Hash 值 M_{i-1}，本次区块头数据 TD，以及 $Nonce$ 值。首先通过一个固定的填充算法使得 $M_{i-1} \| TD$ 的长度为 1600bit 的整数倍。然后将填充过的消息按 1600bit 进行分组，分别记为 $N_0, N_1, \ldots, N_{t-1}$，记 $C_0 = Nouce$。

第一步：迭代计算 $C_j = f(C_{j-1} \oplus N_{j-1})$，其中 $j = 1, \ldots, t$，f 为 1600 比特 Keccak 算法的内部置换，得到 1600bit 的状态值 C_t；

第二步：将 C_t 拷贝 656 份，并按照 128bit 分组成 $T_0, \ldots, T_{8199}$. 记 $Q_0 = AES(T_0)$，然后迭代计算 $Q_j = AES(T_j \oplus Q_{j-1})$，其中密钥值为：

K = 0x123456789abcdef0123456789abcdef0.

第三步：计算 $R_{8198} = aes(Q_{8199} \otimes Q_{8198})$，然后迭代计 $R_j = aes(R_{j+1} \otimes Q_j)$，其中$\otimes$为有限域上的乘法运算，$aes$为 6 轮 AES 算法，密钥同上。

第四步：利用 SHA3 算法计算 $R_0 \| R_1 \| R_2 \| R_3$ 的 hash 值，并输出最低 256 比特。

安全性说明：

Sponge 结构是当前设计密码算法的主流结构，它是针对一个固定置换 f 的迭代过程，可以产生任意长度的输出。CryptoNight 算法采用了 Sponge 结构。

Keccak 算法作为美国 SHA3 计划的获胜算法，其安全性已经得到了密码学界的广泛研究和认可，同时，无论是硬件实现还是软件实现，Keccak 算法都具有一定的优势。目前对 SHA3 算法的原像攻击不超过 7 轮，能转化为实际攻击的不超过 5 轮，由于 Keccak 算法实际具有 24 轮，Keccak 算法可以抵抗原像攻击。

AES 算法是目前使用最为广泛、安全性高的分组密码算法，实际可破译的轮数是 5 轮，CryptoNight 算法采用了完整 10 轮 AES 算法用来扩展消息长度，利用简化 AES 算法实现消息的压缩，有限域上的乘法运算可以有效抵制高概率差分的传播，因此使用 AES 算法及其变形算法，可以有效抵抗各种已知攻击和未知攻击。数据的最终处理交由 SHA3 处理，安全性高。

5.5.2 POS 实现机制

比特币网络全节点锐减的主要原因是缺乏对运行节点的奖励。随着时间的推移，全网接入的用户会更多，对带宽的需求会更高，对节点运行者的资金需求也更多，结果使运行全节点的成本提高。考虑到成本的上升，节点运行者必须要降

低他们的运行成本或者运行轻客户端，但这样完全不利于网络健康。引入主节点技术，能有效地避免主节点减少和传播时间延长等问题。在 Ulord 中，主节点同样是一个全节点，由于考虑主节点候选时考虑了 QoS，通过主节点能快速地传播区块和交易。运行一个主节点，需要 10000 个 UlordToken 和 1TB 以上的存储空间，存储在主节点上的押金不会丢失或损耗，这可让投资者为全网提供服务的同时，赚取一定的投资收益，减少 UlordToken 的价格波动。主节点将获得整个 Ulord 网络 25%的收益。

5.6 其他

5.6.1 隐私保护

Ulord 将采用目前最主流的隐私保护 zk-SNARK 技术保护交易隐私。在比特币的区块链中，创建一笔有效的交易包括以下三件事：

1. 保证地址中的货币没有在之前的交易中花费出去；
2. 发送者通过授权签名的方式证明他自己是这笔货币的“持有者”；
3. 交易的输入与它的输出相等。

证明货币在此之前没有被花费出去的工作是由账本本身完成的，它不需要发送者作出任何工作。发送者仅需证明他是这些货币的持有者，并且他希望通过地址对应的私钥进行电子签名的方式将这些货币发送出去。为了让这个签名得到验证，发送者的地址必须是公开的。与之相对应的，接收者也必须公开接收地址才能完成交易过程。在比特币的使用中，验证交易的输入与输出相等是简单的，因为传输的数量被完全地揭露了出来。

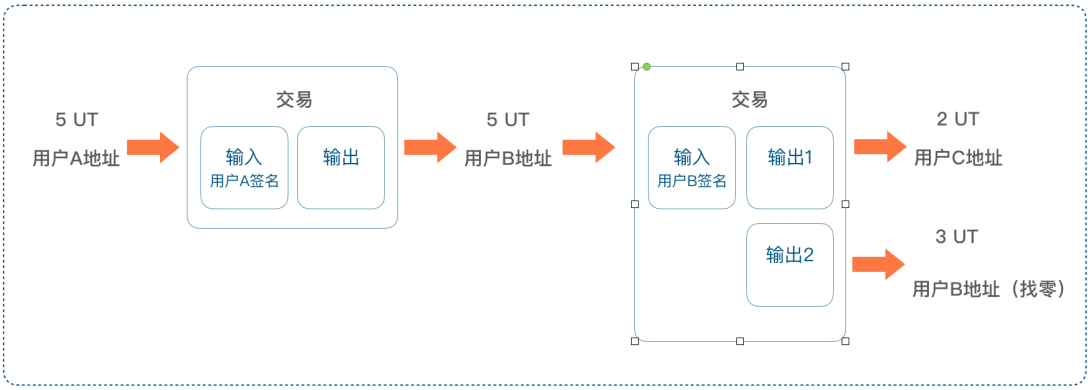

图 9 数字货币交易过程

使用零知识证明（具体来说，zk–SNARKs）来验证以上三个要素可以保护用户隐私不被揭露，即不揭露发送者、接收者和转账数额信息等。每一笔成功的交易都伴随着 zk–SNARK，它证明了：输入的资产是存在的，且之前没有被花费过，创造交易的人授权花费这笔交易，输入的数量和类型与输出的数量和类型相等。在花费输出时需要的信息（也就是创建一个新的 zk–SNARK）被附着在了交易中，通过使用收款人的公钥来加密，仅供收款人使用。

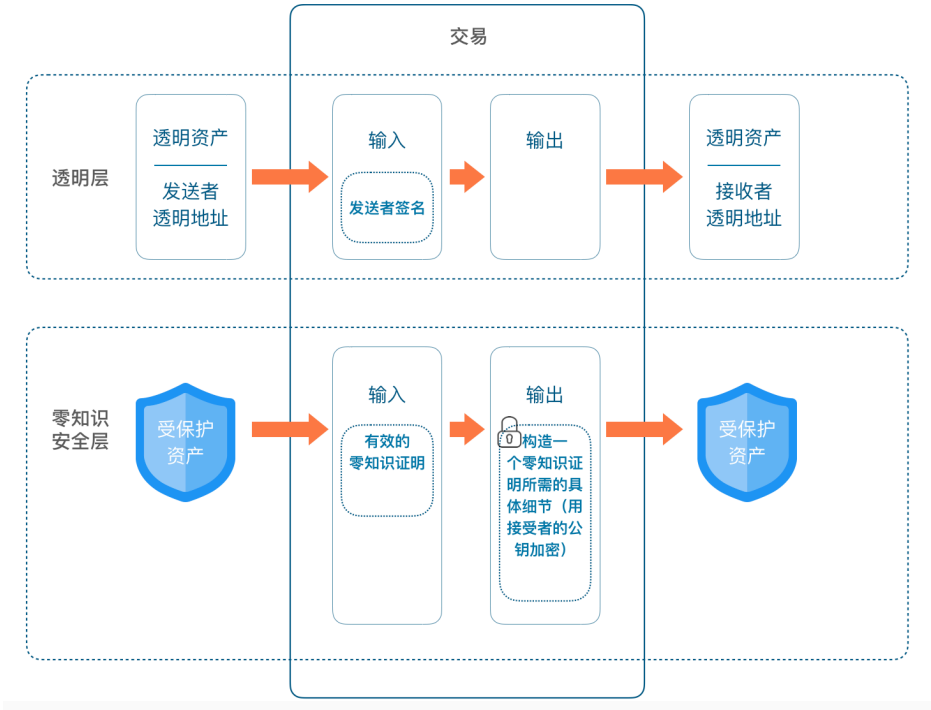

图 10 zk–SNARK 技术保护交易隐私

5.6.2 即时支付

使用主节点技术，用户能够发送和接收即时不可逆转的交易。一旦即时交易形成，该交易的输入被锁定到对应的特定交易去，目前全网交易锁定的时间大约为 4 秒。如果在主节点网络达成锁定的共识，所有与之冲突的交易和区块将被永远拒绝，除非它们能匹配当时锁定的交易对应 ID。

这样，用户可以通过 Ulord 进行商品和服务的购买，满足需要即时支付的商业场景。而且整个支付过程中，没有中心机构的干预。

6 应用设计与实现框架

基于底层“操作系统”和上层“应用程序”的考虑，所有人都可以通过发布者公布出的站点在 P2P 网络中找到自己喜欢的资源，直接从站点获取数据。本章重点对后续的应用规划和参与流程进行简要介绍。

6.1 主要特性

- 实名制

参与到应用平台中的角色都会涉及职责和权益，只有通过实名验证（KYC）的用户才能在系统内发布资源，进行评论或转发，才能获得系统的奖励。实名制可以较好地维护系统的安全与秩序。

- 内容过滤

去中心化不意味着完全无限制的言论自由，对于某些有害的言论和内容（比如色情电影），有必要进行删除和阻止。在 Ulord 体系中，采用基于共识的审查机制（投票系统），让大众来过滤掉不良内容。

- 不可篡改

所有进入发行体系的资源(终稿并通过共识审查)，包括发表的评论或转发，都是不可篡改的，该资源进入区块链时的时间戳，作为最终数字版权确认的依据。相当于基于区块链建立了一个资源发布与传播的存证系统。

- 反垃圾机制

通过“所有信息必须交易”的原则，可以大幅度减少垃圾信息的数量，比如一切盗版或者是没有价值的资源。同时，通过实名制系统设计，盗版或其他不良行为也会让用户在系统中留下不能更改的“记录”，影响用户的信用评级。

- 激励机制

使用者需要为索取的作品支付一些费用（UlordToken），这个费用会随着智能合约的触发而自动分配给了资源发布者和传播者，甚至是高质量的评论者。从另一个角度看，相当于该经济体中的货币回收机制——用于促进体系内的货币流通。

- 应用间交易

在远期的设计考虑中，不同的应用领域可能会有不同的代币，用户可能会同时活跃于各个基于此内容体系下的应用，从而持有各类代币，如果出现这种情况，从机制上支持代币的兑换以及跨应用交易。

6.2 分发机制

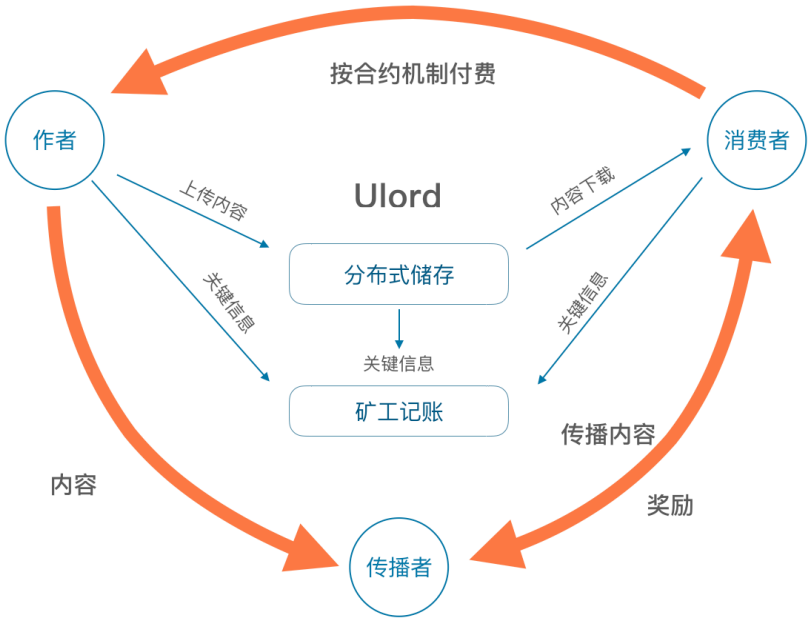

图 11 角色与流程

Ulord 中主要有以下四种角色：

- 版权作者：版权所有者
- 传播者：作品的推广者
- 消费者：作品的受众

- 记账者：矿工

作者可将自己的作品上传、设置分类、填写简介、设置内容时效，并可自行定价。消费者可在平台中搜索自己喜欢的作品及作者，根据分类浏览内容，查看作品简介及用户评论，购买作品，并给购买的作品打分和评论。Ulord 将对数字内容进行加密，通过记账系统，查找发布者，分发消费者付出的费用，当利益分发得到确认后，可以下载获得作品，并将相关数据记录在区块链上。通过 Ulord 的区块链和数据分发体系，资源不仅能被直接提供给消费者，还能依据其本身的质量和受欢迎程度而得到推荐传播。传播者通过存储、转发、推广作品等，按照合约分配各方所得。

上述流程中的主要行为包括：

- 作品发布

作品发布是指作者制作资源并上传至网络的过程。流程如下：

（1）作者创建作品；

（2）Ulord 根据作者的发布申请，生成 AES 秘钥，并对非免费阅读部分的内容进行加密，同时发命令至记账者节点；

（3）Ulord 根据作者的发布申请，生成作品提交交易；

（4）记账者下载发布作品，并发起一个可恢复性凭证交易，确认作品已成功发布。

- 购买作品

购买是指消费者决定购买某些已发布的作品的过程。购买采取合同形式，以消费者的支付承诺开始，以确认记账者已分发作品且消费者向作者完成支付为止。流程如下：

（1）消费者选择想要购买的作品，提出购买申请；

（2）购买申请在平台上生成一个购买请求交易，该交易将有效冻结消费者账户相应数量的数字币；

（3）记账者节点在区块链中发现购买申请后，将使用私钥进行解密，并通过消费者公钥进行重新加密；同时生成分发秘钥交易，包含消费者秘钥加密的份额和交货凭证；

（4）记账者以消费者账户冻结的金额向作者付款；

（5）消费者将会使用其私钥对秘钥份额进行解密，获得作品；

（6）消费者可在区块链中提交一次评级交易，对发布作品进行评论和打分；不同的评级和分类引擎收集这些评级交易，可根据消费者的行为习惯智能推送作品。

- 挖矿

基于以下考虑：

（1）企业/家庭的电脑或其他计算资源使用时间短，使用效率低，迫切愿意将闲置的带宽资源、存储空间、计算资源共享出去，有效利用、资源变现；

（2）参与存储资源的用户（本身可以得到奖励），或者是正在消费使用作品的用户，也可以成为 Ulord 的记账者。

Ulord 设计两种挖矿节点，一种是普通挖矿节点，即企业/家庭的电脑或其他设备，将推出电脑软件挖矿客户端，无需花钱添加其他设备即可在安装软件后成为 Ulord 记账节点参与挖矿，分为智能挖矿、全速挖矿等多种模式，让家庭和办公电脑一机多用，既满足工作娱乐需要，又可以共享资源赚取 UlordToken；一种为专业挖矿节点，在原链设计中已经提及，挖矿算法设计上只适合 CPU 挖

矿，因此可以搭建专业挖矿设备，不同于目前市面上的 GPU 矿机、ASIC 专业矿机，只是 PC 机的简配版，专门为 Ulord 记账，这种节点可能是租用云计算中心的云主机。

这种挖矿模式其实是通过技术创新优化资源使用调度，降低全社会资源消耗，变废为宝，更加绿色环保；从资源分发、传播者的角度看，通过分享有价值的内容，同时也可以参与挖矿获得 UlordToken。

图 12 应用框架

➢ 传播

就版权作品而言，只有被传播、使用的频率增加了，其作品的价值才有可能会提高，一个没有人使用的作品是不具有任何价值的。在互联网时代，每个人都是内容的传播者，大家都有权利表达自己的任何观点，给内容评论、分发或是转载，而由此付出的时间、精力在 Ulord 中同样可以得到报酬，鼓励提供和传播优

质内容。

6.3 UlordToken 分配方案

UlordToken 是 Ulord 平台数字货币，简称 UT，发行总量为 10 亿枚，不可增发也不会销毁。UlordToken 被用于 Ulord 平台的支付，是 Ulord 生态系统中流通货币。UlordToken 的合理分配有利于促进 Ulord 生态系统的健康发展。具体如下：

Ulord 团队及早期投资人：20%，用于 Ulord 所有团队成员及早期投资人贡献奖励。其中 10%为预挖，用于前期项目研发投入；剩余 10%的锁定期为 48 个月，以确保项目能够持续推进。

社区开发者：10%，用于推动社区生态发展，资助开发者执行有意义的开发计划，暂不设定锁定期，会对开发任务进行代码审查和任务质量评估，按完成期限根据社区投票发放奖励。

PoW：35%，激励矿工提供更多的 CPU 算力进行记账。

PoS：25%，奖励给主节点，同时也是鼓励更多的用户提供存储空间用于存储 Ulord 平台上的数据。

社区运营与产品推广：10%，为了让项目能够尽快进入市场，拿出 10%的预算作为早期推广费用。Ulord 会尝试一种社区自治的新模式，所有开支都由社区志愿者共同商议决定。

6.4 如何获得 UlordToken

获得 UlordToken 的方式有下列几种：

（1）CPU 计算资源参与记账；

（2）服务器节点参与网络基础设施建设；

（3）社区推广和代码贡献；

（4）发布原创互联网内容；

（5）传播有价值的互联网内容。

以上方式中，前三种方式是在“生产”环节获得 UlordToken，后两种方式是在“流通”环节获得 UlordToken。UlordToken 资产将记录在 Ulord 的钱包上，拥有 UlordToken 相当于加入了 Ulord 社区，通过社区成员和用户共同努力，促进整个社区生态价值提升。

7 团队

Ulord 团队汇聚了一大批高层次研发人才，由十余名博士领衔，拥有全面的区块链技术应用开发能力。技术开发团队成员有区块链、密码学、互联网信息安全、大数据、云计算、人工智能、金融、管理等多个领域背景的五十多名优秀程序员和算法工程师，顾问团队有顶尖的密码学、区块链领域科学家和行业专家、专业区块链项目投资人，除此之外，Ulord 团队还与加拿大温莎大学、英国曼彻斯特大学、武汉大学、北京航空航天大学、中科院等科研院所保持亲密的合作关系，共同开发 Ulord 平台中的关键技术。

7.1 核心技术团队成员

Dam Woods, CEO, 博士, 近十年来一直致力于云计算方面的研究和开发，具有丰富的带领技术团队开发重大工程项目经验，曾担任某大型云计算中心主任，对区块链行业发展和应用有独到见解。

Kwuaint Li，CTO，博士，一个靠谱的中国程序员。他曾任 Nortel Sigtran 协议的 SME，致力于研究和推广区块链技术。他梦想能在控制区块链技术风险的前提下，将技术红利普惠大众。

Cyber Kuber，CMO，博士，区块链早期投资者，既精通于技术又懂运营的区块链倡导者。他认为区块链将会带领人们建设一个更先进的社会，Ulord 会在这个过程中体现出自己的价值。

Chaoyun Ting，计算机科学与技术专业博士，主要从事人工智能、数据挖掘、区块链等领域的研究，最早从事社交网络研究的学者之一，为社交网络开源社区主要创始人，拥有 8 项发明专利。满怀对世界尖端科技的狂热，Chaoyun

加入了 Ulord，并成为 Ulord 数据分析处理小组负责人。

Yan Xiangtao，博士，美国丹佛大学访问学者。参与完成国家科技重大专项项目 5 项，主持科研课题 3 项，发表科研论文 30 余篇。在项目论证、技术开发和管理协调方面经验丰富，Ulord 项目系统设计小组负责人。

Laktic Lattie，计算机科学与技术专业博士，毕业于武汉大学计算机学院，在大数据挖掘、分布式存储技术等领域方向具有较深积累，参与多个区块链项目的研究与开发，拥有 5 项发明专利，Ulord 项目 P2P 小组负责人。

Cuilin，计算机科学与技术专业博士，参与多个大型分布式系统的设计与开发，在云计算、人工智能、区块链等领域进行了深入研究与实践，有着丰富实践经验，Ulord 人工智能小组负责人。

Zhang Min，法国巴黎第六大学博士，主要从事自然语言处理与机器学习相关算法研究，熟悉各类智能算法的并行加速与优化，在分布式系统故障建模、用户行为分析与内容推荐等方面有丰富的实践经验，Ulord 人工智能小组成员。

Chen Hu，博士，毕业于国防科技大学，华南理工大学副教授，主要从事加密算法、信息安全方向的研究和实现，Ulord 加密算法小组负责人。

Li Mai，加拿大温莎大学博士，麦吉尔大学访问学者。长期从事智能优化算法设计、区块链等领域相关研究，Ulord 系统建模小组负责人。

Liang Liang，管理科学与工程专业博士，在系统评估与优化方法、复杂系统建模、区块链金融等方面进行了较深入研究，在系统软件设计开发方面具有丰富的经验，Ulord 经济模型小组负责人。

Teh Sunn Lau，博士，核心算法工程师，一个来自恰蒂斯加尔邦的区块链狂热分子。他热爱加密算法和热爱爬山一样多。

除了上面团队骨干成员，还有李文宙、周开元、匡冬平、钟云华、屈鹏程、刘秀、胡标、刘齐平、刘必成、苏茗芮、杨昌、郭磊、刘春杰、陈孝经、聂朗、胡庆平、曾学东、陈剑、何进、王璐、舒旭东、郭泰彪、何涛、全松林、曹立楠、邹镇安、罗希、陈韵瑛、彭立彪、尹海波、彭灿、张吕、贺超、刘杨、陈钱、谭科等程序员和算法工程师参与 Ulord 项目研发。这些年轻人充满激情。他们深信区块链将带来一个新的时代，都愿意投身这场技术变革。

7.2 顾问团队

Chris Wood，先后任职澳大利亚某大学计算机科学与软件工程学院副研究员，西班牙某大学计算机科学与数学系高级研究员和研究主任，现为中国某顶级大学教授，博士研究生导师。研究领域涵盖云计算安全、大数据安全与隐私、区块链与数字货币、新兴信息系统安全和应用密码学。

Yu Yong：陕西师范大学计算机科学学院教授，博导，陕西省百人计划特聘教授，中国密码学会青年工作委员会委员，中国密码学会协议工作委员会委员，中国保密协会隐私保护专委会委员。研究方向为公钥密码理论及应用、区块链与密码货币、云计算安全、大数据安全与隐私保护。

Zhang Xiaoming，计算机科学与技术专业博士，原国防科技大学“高性能计算”创新团队成员，现任湖南长城银河科技有限公司首席架构师，曾担任我国“天河”系列超级计算机计算处理系统副主任设计师。

Chen Wenhua，加拿大阿尔伯塔大学博士，在演化计算、机器学习、大数据等相关领域具有厚实的研究基础。在智能优化主流会议 WCCI、CEC、SSCI 等多次组织专题会议，担任会议 Chair，目前是 IEEE TEVC、 IEEE TCYB、Information Sciences、Applied Soft Computing 等 10 多个国际著名期刊的审

稿人。

Jack，INB 资本创始合伙人，区块链知名投资人。投资案例有天河国云、中孚达股份、葫芦堡股份、几维控股、31 会议、Qtum、DEW、Ven、Big1、BeeChat、Mixin、Zcash、EOS、TAMC、AELF、UChain 等。

Feng Tao，多伦多大学数学博士，现任上海永宣创业投资管理有限公司创始人、总裁和管理合伙人。曾入选《财富》全球 25 位企业新星。2009 年 12 月 15 日，被《福布斯》中文版杂志评为“2009 福布斯中国最佳创业投资人”，位列第四。

David Jung，韩国最早的最有经验的区块链挖矿企业 CEO。

Kim Deok-Jung，韩国知名区块链平台和解决方案企业 CEO。

Kim jae-wook，Bithumb CEO。

Cao Wei，于 2010 年 11 月加入蓝驰创投北京办公室，目前任投资董事。他关注的主要方向包括互联网社区、游戏、电子商务及无线应用等。

7.3 投资机构

同道大叔、DFUND 基金、节点资本、千方基金、连接资本、九鼎实验室、优瓠资本。

8 项目推进计划

2016 年 11 月 开启 Ulord 生态建设之旅

2017 年 05 月 完成公链关键技术攻关

2017 年 07 月 完成公链基础工作

2017 年 08 月 搭建信息资源分发平台框架

2017 年 11 月 公链大规模节点测试

2017 年 12 月 基于公链的信息资源分发平台测试版

2018 年 01 月 Ulord 官网 技术白皮书 Ulord 1.0 版本发布

2018 年 03 月 Ulord 2.0 版本发布

2018 年 04 月 推出 Ulord 主节点

2018 年 05 月 完成 AI 核心算法研究与实现

2018 年 06 月 Ulord 3.0 版本发布，提供应用示范

2018 年 08 月 基于 Ulord 公链搭建 5 个以上应用

2018 年 10 月 Ulord 生态体系基本建立

2018 年 11 月 Ulord 4.0 版本发布，进一步提升用户体验

2018 年 12 月 与更多合作伙伴对接各类应用

9 总结

经过深入的行业调研与技术探索后，我们深信区块链技术将为信息资源分发行业打开一扇新的窗户，用去中心化、可信赖的技术和模式去彻底颠覆传统，实现价值高效传递。Ulord 平台将底层区块链服务和 P2P 分布式服务有机融合，为广大用户提供基于区块链的互联网信息资源分发整体解决方案。依托我们在区块链和 P2P 技术深耕多年的经验，我们有信心能够推动技术创新并打造出基于信息资源分发应用的完美生态。

免责声明

区块链作为新兴产业，具有极高的投资风险和技术风险，属于高风险投资行业。白皮书作为技术和产品描述，阐述了技术和产业的布局和前景，不建议没有风险承受能力的人进行投资。

版本声明

不同版本之间表述有矛盾时，以最新版本为准。

解释权

Ulord 基金会对本白皮书保留最终解释权。

参考文献

1. Nakamoto, Satoshi (31 October 2008). "Bitcoin: A Peer–to–Peer Electronic Cash System" (PDF). bitcoin.org. Archived (PDF) from the original on 20 March 2014. Retrieved 28 April 2014

2. EB Sasson, A Chiesa, C Garman. Zerocash: Decentralized Anonymous Payments from Bitcoin. IEEE Symposium on Security & Privacy , 2014 :459–474

3. A Next–Generation Smart Contract and Decentralized Application Platform. https://github.com/ethereum/wiki/wiki/White–Paper

4. Ethereum: A Sercure Decentralised Generalised Transaction RANSACTION Ledger.http://gavwood.com/paper.pdf

5. Dash: A Privacy–Centric Crypto–Currency. https://github.com/dashpay/dash/wiki/Whitepaper

6. CryptoNote v2.0. https://github.com/monero–project/research–lab/blob/master/whitepaper/whitepaper.pdf

7. Kosba A, Miller A, Shi E, et al. Hawk: The Blockchain Model of Cryptography and Privacy–Preserving Smart Contracts[C]// Security and Privacy. IEEE, 2016:839–858

8. Distributed hash table. https://en.wikipedia.org/wiki/Distributed_hash_table

9. BitTorrent. https://en.wikipedia.org/wiki/BitTorrent

10. Wright, A; De Filippi, P. (March 10, 2015). "Decentralized Blockchain Technology and the Rise of Lex Cryptographia". SSRN 2580664?Freely accessible.

11. Levine, M. (17 May 2016). "Blockchain Company Wants to Reinvent Companies". Bloomberg View: Wall Street. Bloomberg News. https://www.bitcoinbook.info/translations/cmn/book.pdf

12. Chao Y, XU M, SI X. Research on A New Signature Scheme on Blockchain[J].

13. Kalodner H, Goldfeder S, Chator A, et al. BlockSci: Design and applications of a blockchain analysis platform[J]. arXiv preprint

arXiv:1709.02489, 2017.

14. Zeilinger M. Digital art as “monetised graphics”: Enforcing intellectual property on the blockchain[J]. Philosophy & Technology, 2016: 1–27.

15. Mastering Bitcoin. https://github.com/bitcoinbook/bitcoinbook.

16. Mastering Ethereum. https://github.com/ethereumbook/ethereumbook.