
Odin Chain 白皮书

写在阅读前：

- 1.没有提高社会效益的企业或组织都应该消亡。
- 2.垄断企业的无良压迫是商业进步的原动力之一。
- 3.公平透明是参与者最基本的保障。
- 4.区块链不但需要保障所有参与者依据贡献获得应有激励，也要惩罚欺诈行为、提高欺诈成本。
- 5.应用落地是区块链良性发展的基础。
- 6.踏踏实实的区块链落地无需站台，站台越多内涵越虚。
- 7.不设顾问，不公布早期投资者，我们不会把利益无端交给任何第三方。

目 录

1. 项目背景 3
2. Odin 链数字广告平台 5
 - 2.1. 互联网广告的问题 5
 - 2.2. Odin 广告公链生态 7
 - 2.3. 项目优势 9
3. Odin 广告公链系统 9
 - 3.1. 设计思想 9
 - 3.2. 系统概述 10
 - 3.3. Odin 浏览器节点：用户节点 12
 - 3.4. Odin 浏览器节点：广告节点 13
 - 3.5. Odin 区块链系统维护节点 13
 - 3.6. Odin 区块链 14
4. 主要技术 15
 - 4.1. 贡献度计算过程 15
 - 4.1.1. 节点类型 15
 - 4.1.2. 记账周期 16
 - 4.1.3. 贡献度计算 16
 - 4.1.4. Odin 记账节点选举 18
 - 4.1.5. 权益分配 18
 - 4.1.6. 交易过程 19
5. Odin 链经济模型 19
 - 5.1. Odin Token 价值基础 19
 - 5.2. 激励机制 20
 - 5.3. 发行机制 20
 - 5.3.1. 发行模型 20
 - 5.3.2. Odin Token 单位 23
 - 5.3.3. 难度 23

5.3.4.	Odin Token 生成	24
5.3.5.	Odin Token 交易的生命周期	24
5.4.	分配机制	24
6.	团队成员	25
7.	进度计划	26
8.	参考资料	28

1. 项目背景

市场研究公司 Magna 预计，到 2020 年全球半数的广告支出将流向在线广告市场，与花费在电视、印刷媒体和广告牌等上面的线下广告支出相当（图 1.1）。Magna 预计，到 2018 年全球数字广告将占市场总体的 44%，规模为 2370 亿美元；到 2020 年在线广告的市场份额将达 50%，规模为 2910 亿美元。当前各种形式的数字广告都在增长，其中搜索广告的股份最大。预计 2018 年，营销商的搜索广告支出将达 1130 亿美元，较 2017 年增长 12%。这些搜索广告支出大部分将花在移动端，占比达 63%。Magna 还预计，2018 年所有类型的移动广告支出将达 1470 亿美元，较 2017 年增长 27%。目前，品牌接触消费者的方式比以往任何时候都多，一些公司正将他们的大部分广告支出分配到线上。

US Total Media Ad Spending Share, by Media, 2014-2020							
% of total							
	2014	2015	2016	2017	2018	2019	2020
TV	39.1%	37.7%	36.8%	35.8%	34.8%	33.7%	32.9%
Digital	28.3%	32.6%	35.8%	38.4%	40.8%	43.1%	44.9%
—Mobile	10.9%	17.3%	22.7%	26.2%	28.8%	31.0%	32.9%
Print	17.4%	15.4%	13.9%	12.9%	12.2%	11.6%	11.1%
—Newspapers*	9.1%	8.0%	7.2%	6.6%	6.1%	5.7%	5.5%
—Magazines*	8.3%	7.4%	6.8%	6.4%	6.1%	5.8%	5.6%
Radio**	8.4%	7.8%	7.4%	7.0%	6.7%	6.4%	6.1%
Out-of-home	4.0%	4.0%	3.9%	3.8%	3.7%	3.5%	3.4%
Directories*	2.8%	2.5%	2.2%	2.0%	1.9%	1.7%	1.6%
Note: *print only; **excludes off-air radio & digital							
Source: eMarketer, March 2016							
205439				www.eMarketer.com			

图 1.1 媒体市场份额占比

Digital Ad Revenue by Company

These companies are expected to be top earners in Internet ads this year.



Tech Chart of the Day

Yahoo's Core Revenue in Perspective

Global advertising revenue of Yahoo, Facebook and Google

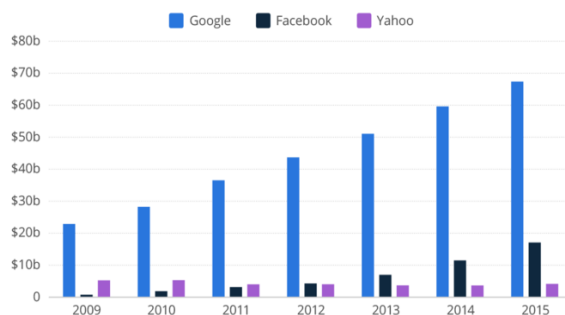


图 1.2 美国主要在线媒体的收入及其变化情况

得益于广告主们在媒体广告领域投入的增加，2017 年，全球媒体广告规模将增长至 5520 亿美元左右，同比增长 3.7%，这一数字虽低于 eMarketer 早期的预测，广告规模却仍然在增长。预计 2020 年在线广告的市场份额将超过广告市场总量的 50%，若加上其它营销服务，全球在线营销服务支出总额预计将首次突破 1 万亿美元。

目前基本所有的互联网巨头都依靠在线广告获得收入。以 Google 为代表的搜索引擎和以 Facebook 为代表的社交媒体的收入逐年增高（图 1.2）。Google，Microsoft，Facebook，Yahoo 等基本垄断了美国的在线广告市场，占全球广告收入的 1/5 左右（Matchcraft 2016，Statista 2016）。Google，Microsoft，Facebook，Yahoo 等巨头基本全部依赖在线广告获得收入。Facebook 和 Google 基本占据了美国在线广告市场 77% 的份额，处于绝对的垄断地位。中国市场的互联网巨头，百度、微博、新浪、搜狐等在线广告的利润占了总营收的 50% 以上。可见，在线广告的市场容量逐渐提高，现有市场容量巨大，并且市场总量急剧扩张。

2014 年以来起，全球广告市场稳步发展，增速保持在 5%~6% 之间，预计一直到 2018 年，广告市场都将保持这样的增幅。全球广告市场主要集中在北美、亚太地区和欧洲三个地区（Emarket 2015）。在短期内，北美仍然是主要的广告市场，但相较于亚太市场而言，其增长规模和速度有下降趋势。未来亚太地区将成为全球广告的主要市场（图 1.3）。

Total Media Ad Spending Worldwide, by Region, 2014-2020 billions and % change							
	2014	2015	2016	2017	2018	2019	2020
Total media ad spending (billions)							
North America	\$184.95	\$192.81	\$202.38	\$212.00	\$223.20	\$234.48	\$245.93
Asia-Pacific	\$147.34	\$158.30	\$171.51	\$185.78	\$202.61	\$219.39	\$235.48
Western Europe	\$93.23	\$95.44	\$97.88	\$100.22	\$102.56	\$104.80	\$106.99
Latin America	\$28.81	\$31.02	\$34.02	\$37.06	\$39.41	\$41.14	\$42.54
Middle East & Africa	\$20.62	\$21.85	\$23.10	\$24.25	\$25.35	\$26.44	\$27.49
Central & Eastern Europe	\$13.53	\$13.65	\$13.67	\$14.04	\$14.57	\$15.22	\$15.81
Worldwide	\$488.48	\$513.07	\$542.55	\$573.36	\$607.70	\$641.47	\$674.24
Total media ad spending growth (% change)							
Latin America	12.6%	7.7%	9.7%	8.9%	6.3%	4.4%	3.4%
Asia-Pacific	9.5%	7.4%	8.3%	8.3%	9.1%	8.3%	7.3%
Middle East & Africa	6.9%	6.0%	5.7%	5.0%	4.5%	4.3%	4.0%
North America	3.3%	4.3%	5.0%	4.8%	5.3%	5.1%	4.9%
Western Europe	2.2%	2.4%	2.6%	2.4%	2.3%	2.2%	2.1%
Central & Eastern Europe	7.4%	0.9%	0.2%	2.7%	3.7%	4.5%	3.8%
Worldwide	5.7%	5.0%	5.7%	5.7%	6.0%	5.6%	5.1%
Note: includes digital (desktop/laptop, mobile and other internet-connected devices), directories, magazines, newspapers, out-of-home, radio and TV Source: eMarketer, March 2016							
206069				www.eMarketer.com			

图 1.3 全球广告市场的变化情况

2. Odin 链数字广告平台

2.1. 互联网广告的问题

当前的网络广告形式主要有文本、图表、音频、视频、超链接、虚拟现实等方式。网络媒体通过展示广告、富媒体广告、文本关联广告、电子邮件广告、文本链接广告、赞助式广告、分类广告、植入广告、社交媒体、视频网站等方式传递广告信息。虽然网络广告已经被广泛接受，成为市场中的主要宠儿，其份额也逐年提升，市场潜力巨大，但是网络广告仍然存在一些问题（图 2.1）（Aksu et al. 2018）。

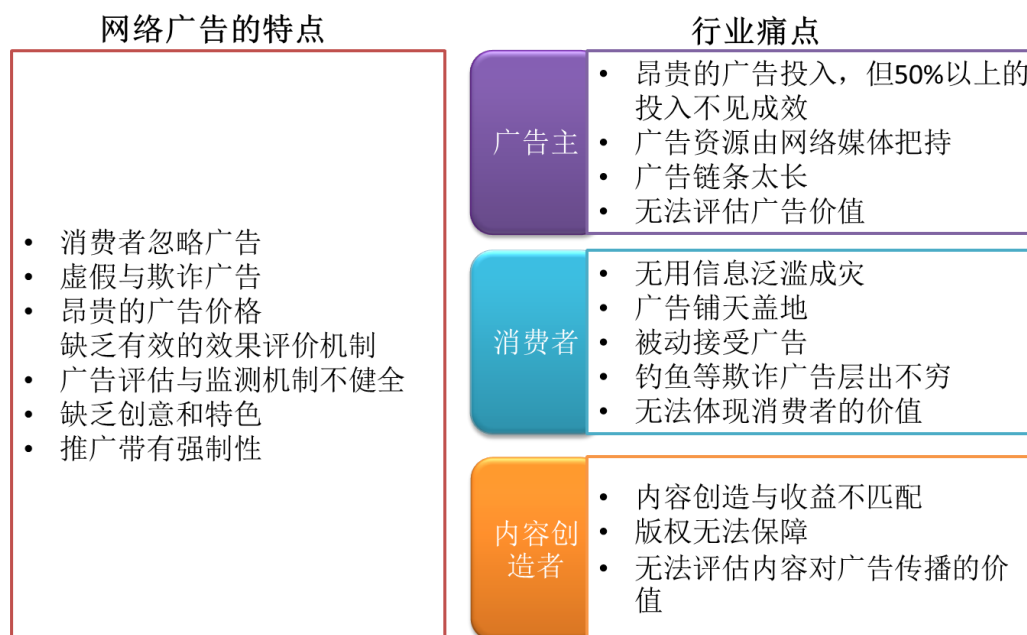


图 2.1 网络广告的特点及行业痛点

(1) 消费者忽略广告。消费者习惯于在电视上看到广告，在广播中听广告，在翻阅杂志中阅读广告，他们对各种形式的广告产生了反感。在线广告也是如此，消费者可以避免点击横幅广告，在在线视频中绕过广告，一旦他们在屏幕上出现，就会关闭弹出式广告。客户控制着要单击并响应的广告信息。

(2) 虚假与欺诈广告盛行。在传统广告的管理中，从事广告业务有一定的市场准入条件，要通过广告业的资格认证，获得营业执照，这使得对广告的监管有法可依。但在网络的虚拟环境中，由于缺少这一准入制度，几乎任何拥有网络使用权的企业、其他经济组织或个人都可以从事广告业务，使得网络广告的管理非常困难。此外，网络广告法律规范的缺失给虚假、欺诈性广告提供了可乘之机，造成了网络广告行业的混乱，严重损害了网络广告的公信力。

(3) 广告价格昂贵。网络广告通常按照 CPS，CPA，CPC，CPM 等进行定价（Miralles-Pechuán et al. 2016），例如以 CPA 进行定价，每次点击的平均价格为 2.5 美元，若在《纽约时报》这样的热门网站上做广告，每个月的广告费用则在上千美元以上。广告的成本根据网站、博客接收的流量和读者类型的不同而有所不同。按点击付费活动和社交媒体网站进行在线广告，也会对公司的营销预算造成严重破坏，这可能对投资没有回报。

(4) 缺乏有效的效果评价机制（Miralles-Pechuán et al. 2016）。CPM 和 CPC 作为广告主衡量互联网广告效果和支付广告费用的两个重要指标，在 Web2.0 时代显得有些片面，因为广

告主更想精确了解哪些消费者在关心他们的产品和服务，或者对他们产品和服务的哪些部分感兴趣。他们希望了解消费者从认知到认可整个心理变化的过程和特征，从而指导网络营销体系的完善。而且，用户的点击冲动与很多因素有关：创意表现的新颖性、广告词的煽动性、对产品的兴趣、活动的奖品设置、产品代言人等等都影响着点击的数量。

(5) 缺乏创意和特色，推广带有强制性。在美国心理学家吉尔福特提出的智力三维结构模型中，信息内容被分为五种类型：视觉（V: Visual）、听觉（A: Auditory）、符号（S: Symbolic）、语义（M: Semantic）和行为（B: Behavioral）（Guilford 2011）。和传统的其他三大媒体相比，惟有第四媒体可以实现 V+A+S+M+B 多种信息内容呈现方式的综合，这为网络广告提供了强大的发布平台，但是由于网络带宽不足和创意、制作水平不高，我国网络广告的表现形式比较单调，以传统的旗帜式、按钮式广告、电子邮件居多，而且往往采取强制性的信息推送手段，导致网络受众体验很差。

(6) 网站作恶。对点击次数等指标造假，实现流量欺骗，骗取广告主高额广告费用。

(7) 广告评估与监测机制不健全。专业的评估包括两方面：首先是量的评估，比较计划和执行在量上的区别；其次是研究广告的衰竭过程，将同步广告每天的点击率在坐标平面上连线，确认每个创意的衰竭时间，为设计广告创意更换间隔提供依据。因此，网络广告评估是衡量广告效果的基本手段，也是广告主投放中长期广告的主要依据。

2.2. Odin 广告公链生态

为解决前述互联网广告存在的问题，我们基于区块链技术、智能合约设计了 Odin 广告公链。在它的基础上可以开发去中心化的浏览器应用，广告主可在浏览器上投放广告，浏览器使用者可选择是否浏览广告，双方通过智能合约制定协议有机结合在一起。

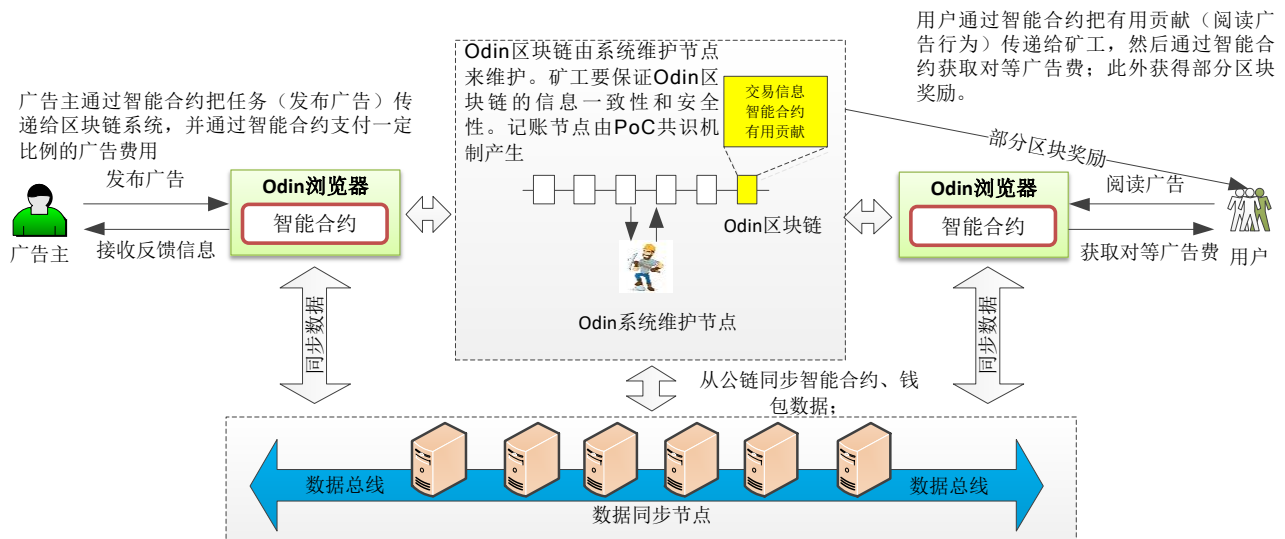


图 2.2 Odin 广告公链生态系统

如图 2.2 所示，广告主和浏览器使用者首先注册成为公链用户，获得一对公钥和私钥，然后注册成为浏览器用户。广告主在浏览器上设定好智能合约内容（广告发布和基于广告浏览量的奖励分发协议），用私钥签名后发布到公链上，浏览器使用者从公链上同步数据后，可选择是否与广告主签订智能合约。如果使用者需要签约，则只需用自己的私钥在合约中签名，然后浏览器会把合约以函数调用的形式，广播到 Odin 系统中。系统维护节点接收到合约之后，会解析智能合约，把智能合约中的内容解析出来，打包到新区块中。新区块创建完会被广播到 Odin 系统中，等大多数挖矿节点达成共识后被添加到区块链中。在智能合约中包含的主要参数有：广告覆盖的地区范围（Range）、广告发布周期（Period）、广告费用（Bonus）、广告需返回的参数（Returns）、基于广告浏览量的奖励分发协议等。若智能合约用 adSmartContract 表示，那么智能合约将携带参数发布到 Odin 系统中，Odin 系统维护节点会解析智能合约并创建新的区块，形式表达如下：

Odin 系统维护节点 <- adSmartContract (Range, Period, Bonus, Returns)

不同的角色通过智能合约，主动选择自己的意愿条件，将不同的参数通过智能合约传递给 Odin 系统。Odin 系统维护节点在确认智能合约的有效性后，达成共识创造新的区块，区块内合约的执行使得信息的价值可以在用户间传递。整个过程是公开透明且不可篡改的。

区块链将记录交易信息、智能合约和广告浏览数据等信息，并保证信息的一致性和安全性。Odin 系统维护节点是系统数据的维护者，它负责保证数据的一致性和安全性。

2.3. 项目优势

Odin 广告公链：基于区块链技术的数字广告平台。

Odin 浏览器：基于 Odin 广告公链研发的去中心化浏览器——现行流量垄断机构的破局者。

与传统的网络广告平台相比，Odin 项目具有如下优势：

- 用户是 Odin 浏览器的使用者，将享有屏蔽和阅读广告的权力，主动阅读广告将获取相应的 Token 奖励。
- 智能屏蔽不良广告，让用户在安全防护网下进行网上冲浪。
- 屏蔽广告及替换采用插件实现机制，由第三方开发者提供，具备灵活扩展能力。
- 广告流通过程公开、透明，广告主将很清楚地知晓每一笔广告费用流向何处。
- 数据真实可靠，有助于广告费用的评估。为了获得 Token 收益，用户将会把阅读广告的行为数据对广告主公开，广告主将得到用户阅读广告的相关数据，进行深度分析，从而评估广告的效果。
- 人人都可以成为广告运营商，只要其具有运营广告的能力，就可以根据其业绩获取 Token 收益。
- 采用去中心化、独立公链系统管理模式，保证收益公平。
- Odin 浏览器通过软件充分保护用户隐私，保证信息真实可溯源。

3. Odin 广告公链系统

3.1. 设计思想

- (1) 数据可靠性和一致性。数据一致性其实是数据库系统中的概念，可以简单地把一致性理解为正确性或者完整性。而在分布式系统中，数据一致性往往指的是由于数据的复制，不同数据节点中的数据内容是否完整并且相同。
- (2) 可迁移机制。Odin 节点会随着用户的流动增加、转移和退出。系统要保证增加 Odin 节点时，能够扩充系统的边界，正常地运行，并且能够在一个记账周期内根据 Odin 节点的贡献，分配相应的权益。同理，当 Odin 节点从系统中移除时，

不影响信息的传播、记账等功能，从而保证系统可伸缩。

- (3) 轻客户端。为了减轻 Odin 节点的工作强度，Odin 节点的客户端分为两类：Odin 数据同步节点和 Odin 浏览器节点。Odin 数据同步节点负责数据的实时同步、更新，Odin 浏览器节点调用距离其最近的 Odin 数据同步节点中的数据，从而实现快速响应。
- (4) 滞后结算策略。分布式交易体系的问题在于收款人很难校验之前的某位资产所有者是否进行了双重支付（双花）。通常的解决方案是引入可信的第三方，如银行，来对每一笔交易进行检验，以防止双重支付。而如果想要排除第三方中介机构，那么交易信息就应当被公开，需要整个系统内的所有参与者，都有唯一公认的历史交易序列。因此，采用滞后结算交易的方式，通过记账节点对账来排除双重交易，保证交易在交易期间内是首次出现的。
- (5) 权益锁定。为消除记账节点迁移和撤出 Odin 系统带来的负面影响，维护系统的可靠运行，当记账节点获取到相应的权益后，会对其权益进行锁定，在一定时间内，这些权益不能进行交易。待记账节点的服务达到一定时间后，不再影响 Odin 的正常运行，此时开始解除锁定。解除锁定后，用户可以自由交易权益。权益锁定期内，记账节点也能够获取相应的利息。
- (6) 快速达成共识。分布式交易体系的问题在于收款人很难校验之前的某位资产所有者是否进行了双重支付（双花）。
- (7) 价值共识与激励。只要 Odin 节点贡献自己的能力给其他节点，那么它就可以获取对等的权益；并且 Odin 节点在网络中存在的时间越长，获得的权益也越多。

3.2. 系统概述

尽管区块链技术有一定的瑕疵（Eyal 2015, Eyal and Sirer 2013, Nayak et al. 2016）（AZURE 2016, CACHIN 2016, ROSS and SEWELL 2015），但区块链技术（Garay, Kiayias, and Leonardos 2015, Nakamoto 2008）（2016）作为创造信任的机器，具有分布式结构、建立信任、公开透明和时序不可篡改等技术优势，吸引了金融界和工业界的广泛关注，并开始被用于重塑交易系统，在降低交易成本和提高交易效率方面效果显著。

工作量证明（Proof of Work, PoW）（Nakamoto 2008）是当今去中心化加密算法中最稳健的共识机制。PoW 主要用于选取一致的领导力节点，并给参与者合适的奖励。在区块链系统中，作为共识机制的参与者，系统维护节点能够根据其算力被竞选为领导力节点。有了算力成本的约束，就可以防止伪装成多节点的大算力攻击者，相应的代价就是要消耗大量的算力。算力消耗是基于工作量证明（Proof of Work, PoW）构建的区块链系统的问题所在，大量的系统计算资源和电能被耗费，使得系统的扩展性受到制约。

在 2011 年早期，权益证明 PoS（Proof of Stake）的概念被提出（Houy 2014）。直观地说，权益证明就是拥有 Token 量证明的一种形式，Token 零消耗是权益证明的一种形式。因此，权益证明被用在 ppcoin 中，并用来改进 PoW 工作机制耗费电能的缺点，且不容易被伪造。2014 年，以太坊设计了以太坊 PoS 架构，被称为友善小精灵 Casper（Casper the Friendly Ghost）（Houy 2014），是一种 PoW 协议的 PoS 变种。在以太坊系统中，只有在验证人缴纳保证金的情况下，他的签名才有意义。客户端智能依赖于出自当前锁定保证金的验证人的块。已知当前锁定保证金的验证人，就可以鉴别出共识认可的链。不知道现在交纳保证金的验证人列表的客户端，必须先通过另外的信道获取这个列表，这个限制通过要求所有人用当前信息鉴别共识解决了“远程攻击”问题。

为了解决 PoW 的挖矿效率低下和消耗资源的问题，我们结合浏览器用户访问浏览器的行为（可以理解用户对 Odin 系统的有用贡献，useful contribution，简称“贡献”）和区块链技术，设计和构建 Odin 系统。在工作量证明的过程中充分考虑浏览器用户的贡献，实现了用户贡献+工作量证明的算法。为了降低系统的工作量，在节点选举过程中使用浏览器投票的方式（图 3.1）。

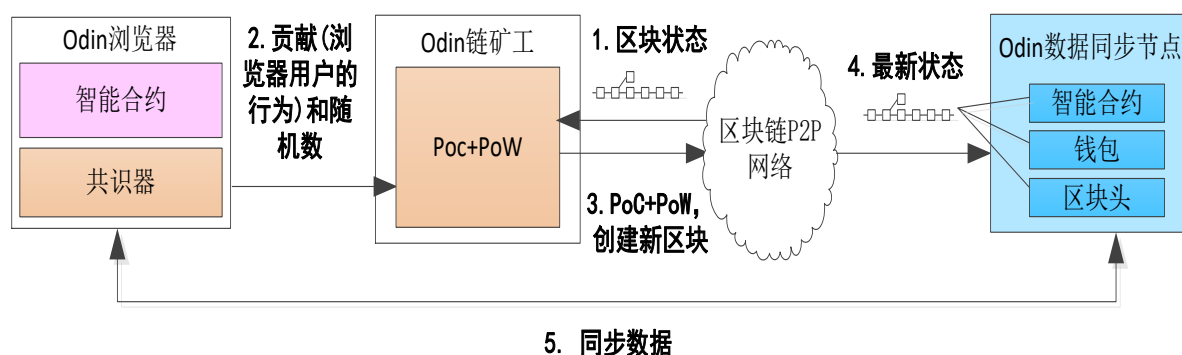


图 3.1 Odin 系统结构概述

Odin 生态系统包括浏览器用户、广告主、Odin 链系统维护节点和 Odin 数据同步节点。

- **Odin 浏览器节点：用户节点。**用户通过私钥签发智能合约，向 Odin 系统发布用户行为数据，用于证明自己对系统的贡献，根据其贡献获取对等的奖励（包括：**广告主支付的广告费和挖矿奖励**）。智能合约将封装浏览器的用户行为数据和随机数，并打包成一个区块，加密后广播到区块链系统中，等待系统维护节点的验证。
- **Odin 浏览器节点：广告节点。**广告主使用智能合约在浏览器上发布广告，并把合约信息封装后发送给 Odin 链系统维护节点。Odin 链系统维护节点对信息进行解析，并对信息进行验证，验证完成后打包到新区块并将其广播到网络中。
- **Odin 链系统维护节点：**即 Odin 链矿工，是验证浏览器用户贡献的重要节点，它使用贡献度证明（Proof of Contribution）+工作量证明（Proof of Work）的机制，验证 Odin 浏览器节点的贡献，并将最终产生的新区块广播到 P2P 网络之中，实现系统共识。此外 Odin 矿工会把发送到公链上的交易和智能合约打包到新区块中。
- **Odin 数据同步节点：**一般为小型 PC，从公链同步下载最新智能合约数据和用户钱包数据到节点上，方便附近的终端用户同步下载相关数据。

3.3.Odin 浏览器节点：用户节点



图 3.2 Odin 浏览器整体框架图

用户节点通过阅读广告，触发与广告主之间签智能合约的动作，成为某个广告传播的贡献者。用户通过 Odin 浏览器节点，把其贡献和浏览器生成的随机数通过智能合约封装，最后加密打包生成区块广播到网络中，等待系统维护节点统计并返回某个广告的激励和部分区块奖励。假设随机数是 RandNum，贡献是 UC，Odin 浏览器客户端将对这些参数进行封装，签署智能合约，并广播到区块链系统中。形式如下：

Step1: 调用智能合约封装贡献，返回 SC， $SC \leftarrow \text{SmartContract}(\text{RandNum}, UC)$

Step2: 通过浏览器客户端发送封装后的消息，例如： $\text{SendtoBlockchainsevers}(SC)$

Step3: 通过浏览器客户端不断监听数据同步节点的数据，以更新钱包等信息。

3.4.Odin 浏览器节点：广告节点

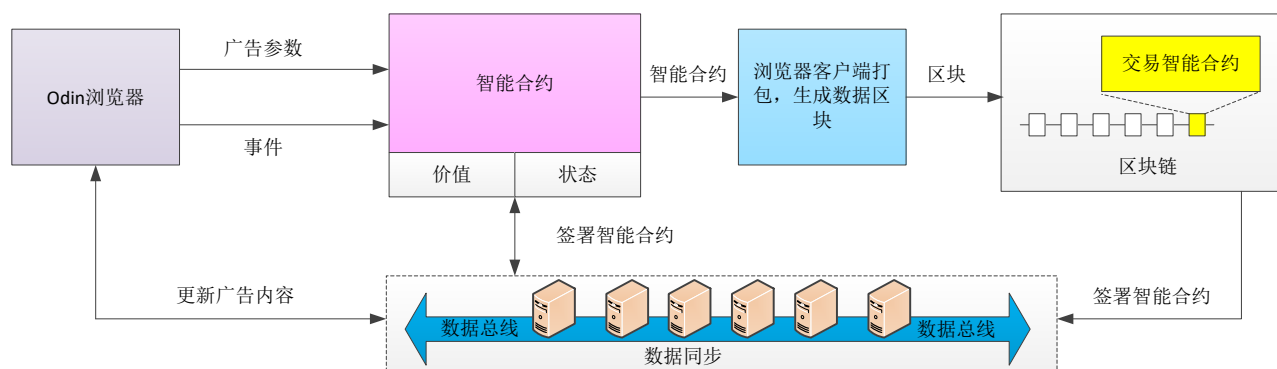


图 3.3 Odin 浏览器节点系统结构及其模块调用流程

广告主通过发布广告，触发与用户之间签智能合约的动作，成为广告传播的雇主。广告主通过浏览器发布广告，把广告发行周期、范围以及广告奖励等参数通过智能合约进行封装，然后通过浏览器生成数据区块，广播到网络之中，并寻求系统维护节点，把广告信息写到区块链系统中。当广告信息被写入区块之后，就会把信息广播到数据节点，数据节点与广告主签署智能合约，同步广告内容，等待浏览器用户的访问。假设广告主发布广告需要传递的参数有 period, place 和 price, 智能合约将把这些参数封装，签署智能合约，并广播到区块链系统中。形式如下：

Step1: 调用智能合约封装广告参数，返回 SC，例如：SC<-SmartContract (RandNum, period, place, price)；

Step2: 通过浏览器发送封装后的消息，例如：SendtoBlockchainsevers (SC)

Step3: 增加区块并验证区块的有效性，例如：AddBlock () and Validation ()

Step4: 数据同步节点与广告主签署智能合约，SignSmartContract ()

Step5: 同步广告数据 DataSynchronization ()

3.5.Odin 区块链系统维护节点

Odin 区块链系统维护节点构建系统共识，保证数据的一致性和安全性。为保证 Odin 系统维护节点的权益，保证其能够公平地参与记账权的分配并公平参与区块的产生，所有 Odin 浏

浏览器用户产生的有用贡献与随机数一起广播到网络中。Odin 系统维护节点捕获浏览器用户的贡献信息后，将解析 Odin 浏览器给的随机数，由此来判断是否由自己来计算贡献度值。用 RandNum（Useful contribution）表示 Odin 浏览器产生的随机数形式如下：

$$\text{Odin 系统维护节点地址} = \text{hash}(\text{RandNum})$$

只有当随机数的 hash 运算结果与 Odin 系统维护节点地址相同时，该节点才获取节点数据统计权。

同时，为了让贡献度能够影响系统维护节点的挖矿能力，在工作量证明的同时，引入贡献参数。假设用 D（Difficulty）表示当前挖矿难度，用 UCs（Useful Contributions）表示系统维护节点统计的贡献总和，当且仅当当前系统维护节点的 UCs 高于 80% 的系统中的其他系统维护节点（目的是让 1/5 的算力参与挖矿，剩余 4/5 算力继续同步数据，避免算力浪费）时，才将有资格进行工作量证明，即：

$$\text{OdinProof}(\text{UCs}, \text{D}, \text{hash}, 20\%)$$

与 PoW 相同，当且仅当其解 hash 值的速度最快，将会获取创建新块、记账的权利。

3.6. Odin 区块链

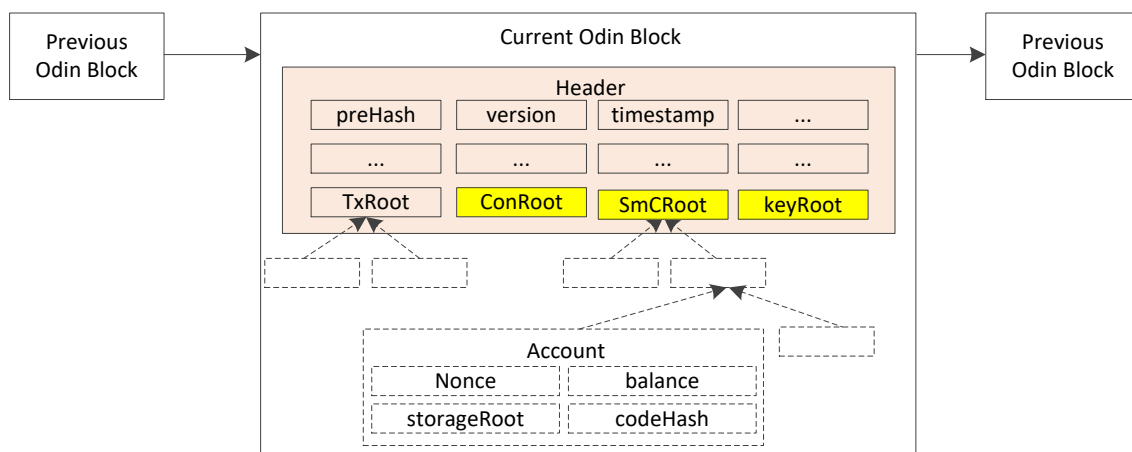


图 3.4 Odin 链的区块形式

参考以太坊的区块头来设计 Odin 链的区块头（Wood, 2014），Odin 区块头封装了父块 Hash、版本号、系统维护节点地址、区块序号（高度）、Bloom 过滤器、当前 Token 总量、Token 使用量、难度级别、附加数据、混合摘要、随机数、交易根、状态根以及收据根等信息，其中交易根、贡献（Contributions Root）根、智能合约（Smart Contracts）根、密钥根分

别是交易树、有效贡献树、智能合约树的根节点 Hash 值，而交易树、贡献度树和密钥树是由 Merkle Patricia 树构造而成的。交易列表保存 Odin 链交易信息，贡献度树保存 Odin 链的贡献度数据信息，这与比特币和以太坊的区块结构类似（Nakamoto 2008，Wood 2014）。

Odin 链系统维护节点和 Odin 数据同步节点对于历史区块链信息的需求不同。Odin 系统维护节点在挖矿过程（记账过程）中需要链上的所有信息，它们会同步下载整条 Odin 链，从创世纪块到当前块，执行或校验其中包含的所有交易、贡献和智能合约。Odin 数据同步节点仅仅下载 Odin 链的头（从创世纪块到当前 Odin 块的头）、智能合约、钱包状态数据和广告内容等数据，不执行任何的交易或检索任何相关联的状态。由于 Odin 数据同步节点可以访问块的头，而头中包含了 3 个树的 Hash，所有 Odin 数据同步节点依然可以很容易生成和接收关于交易、贡献度和智能合约三类信息的可验证答案。

取得记账权的 Odin 系统维护节点将当前 Odin 块链接到前一 Odin 块，形成最新的区块主链。各个 Odin 块依次链接起来，形成了一条从初始 Odin 链到当前区块的最长主链，从而记录了 Odin 链数据的完整历史，能够提供 Odin 链数据的溯源和定位功能，任意数据（包括交易信息）都可以通过此链式结构顺藤摸瓜、追本溯源。如果短时间内有两个 Odin 链节点同时算出两个新的 Odin 块加以链接的话，Odin 链主链可能会出现暂时的“分叉”现象，其解决方法是约定 Odin 链节点总是选择累计贡献率最大的 Odin 链。

4. 主要技术

4.1. 贡献度计算过程

4.1.1. 节点类型

在 Odin 链中，根据节点在网络中的作用，把节点分为轻节点和重节点。轻节点包括 Odin 浏览器节点和 Odin 数据同步节点，重节点包括 Odin 系统维护节点。Odin 浏览器节点是安装 Odin 浏览器的客户端，用户可以通过 Odin 浏览器贡献广告阅读行为数据。Odin 数据同步节点负责同步最新智能合约、钱包数据和广告数据。Odin 系统维护节点则负责计算 Odin 浏览器节点的贡献度和记录节点之间的交易行为，它是具有一定计算能力的服务器。

4.1.2. 记账周期

贡献度记账周期是指 Odin 链统计贡献度的周期。自 Odin 链开始运行，每隔一个贡献度记账周期，将会选举一个或多个 Odin 系统维护节点来统计 Odin 浏览器节点的贡献度，并分配 Odin 权益给 Odin 浏览器节点。贡献度记账周期不宜设置过短，周期太短会使得系统中的节点频繁地统计贡献度，消耗大量的计算资源。贡献度记账周期也不宜设置过长，过长的记账周期会降低贡献者的积极性，不利于 Odin 链的建设。

交易记账周期是指对 Odin 链中交易记账的周期。自 Odin 链开始运行，每隔一个交易记账周期，将会选举一个或多个 Odin 链节点来统计 Odin 节点之间的交易数据，保证不会出现双重支付。相对贡献度记账周期而言，交易记账周期更短。过长的交易记账周期会使得系统中的交易不能够快速确认，不利 Odin Token 的流通。

4.1.3. 贡献度计算

(1) Odin 浏览器节点贡献度计算过程

Odin 浏览器节点贡献阅读行为流量，然后把流量广播到网络中。Odin 系统维护节点捕获 Odin 浏览器节点广播的流量数据，然后根据流量计算各 Odin 浏览器节点的贡献度，并按贡献度比例分配广告费用和区块奖励给浏览器节点。在此过程中 Odin 系统维护节点会打包贡献度信息到新区块中，并记录到区块链中。

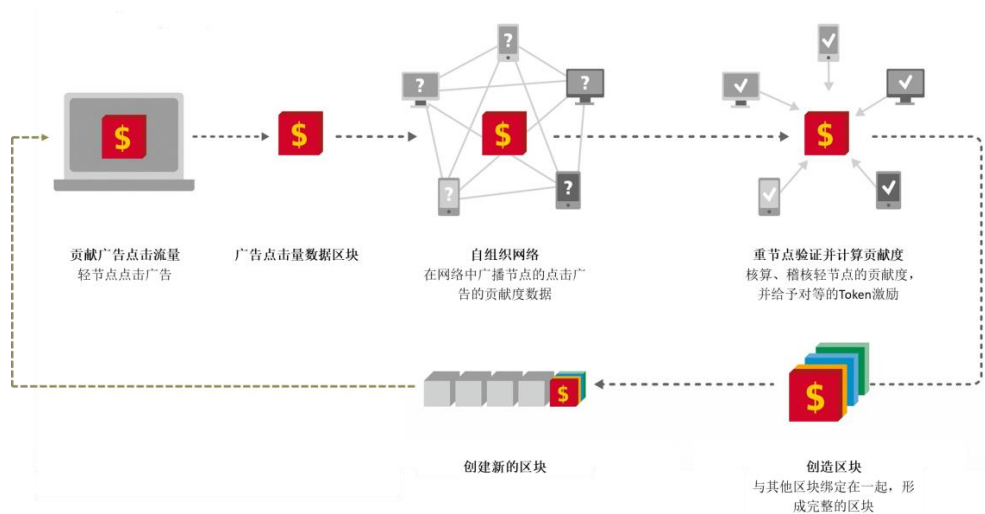


图 4.1 Odin 浏览器节点贡献度计算过程

例如（图 4.1）中：用户在浏览器中点击广告是一种用户行为，Odin 浏览器会记录该行

为数据并打包、广播到 P2P 网络中，等待重节点挖矿。重节点捕获到该信息后，根据用户的行为判断其对广告的贡献支付广告费，同时进行系统激励。

(2) Odin 浏览器节点贡献度计算

假设 1: Odin 浏览器节点阅读广告的行为是人为、主动和真实的广告阅读行为，而非机器、被动和欺骗的广告阅读行为。

假设 2: Odin 浏览器节点阅读广告达到一定数量后，其阅读广告所获取的信息边际递减，其阅读广告的效果效用边际递减。

在假设 1 和假设 2 成立的情况下，我们可以根据 Odin 浏览器节点在一个记账周期内的广告阅读行为（actions）来计算该 Odin 浏览器节点的贡献度，并定义关于贡献行为的效用函数，用来计算 Odin 浏览器节点在 T 时刻的贡献度：

贡献度是关于阅读广告行为或流量的函数。

图 4.2 效用函数曲线

可选取凸函数、凹函数或者线性函数作为效用函数。若广告阅读行为较为平均，可以选取线性效用函数。若系统中存在刷广告阅读行为次数行为的 Odin 浏览器节点，为了防止这些节点刷广告阅读行为量的行为，可以采用凹函数作为效用函数，即随着广告阅读行为次数的增加，这些节点因广告阅读行为次数增加带来的贡献度增量降低至 0。

$$\frac{\Delta Contribution(T)}{\Delta clicks} \rightarrow 0$$

为了鼓励浏览器节点长期、稳定地贡献，增加对 Odin 公链的黏性，引入贡献度年化利息 θ 的概念。Odin 浏览器节点使用 Odin 链软件的时间越长，其获得的收益越高。Odin 浏览器节点在 T 时刻的复利贡献量记为 $WContribution(T)$ 。设贡献度记账周期为 Δt_c 天，T 时刻 Odin 链节点的贡献量为 $Contribution(T)$ ，之前的贡献量为 $Contribution(t)$ ($t = 1, 2, \dots, T-1$)，年化利率为 θ ，那么 T 时刻 Odin 链节点的复利贡献量 $WContribution(T)$ 定义为：

$$WContribution(T) = Contribution(T) + \sum_{t=1}^{T-1} Contribution(t) \cdot \left(1 + \theta \cdot \frac{365}{\Delta t_c}\right)$$

其中 $\theta \cdot \frac{365}{\Delta t_c}$ 是 Odin 链 Odin 浏览器节点持续为系统贡献广告阅读行为或流量获取的额外收益，

相当于 Odin 浏览器节点的贡献率利息。

4.1.4. Odin 记账节点选举

Odin 链中的记账节点必须要有足够的计算能力、存储空间和带宽才有资格被选举为记账节点。假设记账周期产生的数据总量 (Data Volume) 共计 X 千字节, 若 Odin 链节点的计算能力 $\leq X$ 千字节, 那么该 Odin 链节点将不具有资格参选记账节点。与 PoS 的思想相似, 重节点代表一系列浏览器节点的权益, 其代表的浏览器节点越多, 被选择作为记账节点的可能性越高。假设 T 时刻 Odin 链节重节点 i 记录的复利贡献量总量为 $iTWContribution(T)$, 那么它是否有资格记账由下面的公式来确定:

$$\text{记账权资格} = \begin{cases} 0, & \text{if } iTWContribution(T) \leq \pi \\ 1, & \text{if } iTWContribution(T) > \pi \end{cases}$$

π 是贡献度的阈值, 用来确定记账资格, 选出少数的具有记账能力的记账节点。可以选取 20% 的重节点来记账, 并通过 PoW 挖矿机制来从 20% 的重节点中选出记账节点。

4.1.5. 权益分配

被选举来记账的 Odin 系统维护节点将同步所有其他 Odin 系统维护节点的贡献量数据, 并统计 T 时刻 Odin 链所有 Odin 浏览器节点的总复利贡献量 $WContribution(T)$, 它等于所有 Odin 链节点的贡献量之和, 即:

$$TWContribution = \sum_{i=1}^n iTWContribution(T)$$

其中 $iTWContribution$ 为第 i 个 Odin 系统维护节点记录的总贡献量, n 为总的 Odin 系统维护节点数。

假设 T 时刻所处的周期待分配的 Odin 权益总量为 $OdinToken(T)$, 那么第 i 个 Odin 浏览器节点根据其贡献量获得的 Token 权益数量为:

$$OdinToken(T \vee i) = \frac{WContribution(T \vee i)}{TWContribution} \cdot OdinToken(T)$$

在完成权益分配之后, 记账节点将把计算结果封装到贡献度记账区块中, 并广播到网络中, 待其他记账节点验证后获得记账奖励。

4.1.6. 交易过程

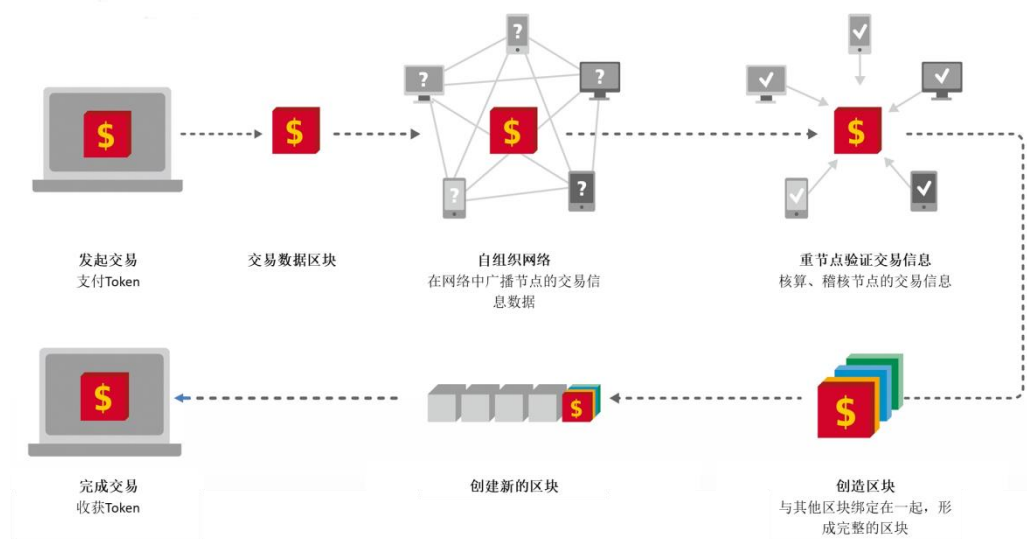


图 4.3 交易过程

交易是指 Odin 链节点之间的资产转移行为。定义 UTXO（Unspent Transaction Outputs）是 Odin 链节点未花费的交易输出。交易构成了一组链式结构，所有合法的 Odin 链节点交易都可以追溯到前向一个或多个交易的输出，这些链条的源头都是挖矿奖励，末尾则是当前未花费的交易输出。

当节点发起交易，会把交易数据打包并广播到网络中。Odin 系统维护节点捕获其他节点的交易数据后，将核算、稽核节点交易信息，并创建区块。区块创建完成后，交易将被确认，并完成。为了防止 Odin 系统维护节点的交易存在欺诈等行为，Odin 系统维护节点只能通过计算贡献量和交易手续费获取收益，它不能参与任何交易。

5. Odin 链经济模型

5.1. Odin Token 价值基础

Odin Token 是 Odin 链上的原生资产，Odin Token 的价值起源是其能够方便地表征和度量 Odin 链上的数字化经济活动。Odin Token 既代表 Odin 链的所有权，又代表其使用权：使用

Odin 链投放广告需用 Odin Token 支付一定的费用，体现 Odin Token 的使用权特性；持有 Odin Token，代表拥有 Odin Token 的一部分，相当于 Odin 链的股东，能够参与到 Odin 链治理的最高决策，体现 Odin Token 的所有权特性。

5.2. 激励机制

Odin 网络包含其内建的 Odin Token，在网络内包含一种 Odin Token 的原因是多重。首先，区块中新发行的部分 Odin Token 被奖励给系统维护节点以促进网络安全；其次，区块中新发行的部分 Odin Token 和广告主支付的广告费被按贡献度比例奖励给用户，以激励用户使用 Odin 浏览器浏览广告，促进网络生长；最后，用它来支付是一种反欺诈机制。类似 Hashcash 的以交易为单位的工作量证明和放任自由是收取交易费的两个替代方案，前者浪费资源并且对于低档计算机和智能手机是不公平的，后者将会导致网络立刻被无限循环的“逻辑炸弹”合约淹没。

此外，还要设定惩罚规则，以便规范用户的广告浏览行为，避免恶意浏览行为产生。

5.3. 发行机制

5.3.1. 发行模型

Odin 系统按节点数量的变化分为上线期、成长期和稳定期。在上线期通过创世区块发行 4M 个 Odin Token，然后每年增加供应量 $p(t)*M$ ，其中增长系数如下：

$$p(t) = \begin{cases} p_0, & t = 0, 1, 2 \\ \left(2 - \frac{(t-1)^\alpha}{(t-2)^\alpha}\right) * p(t-1), & t \geq 3 \end{cases}$$

随着时间 t 增大， $p(t)$ 逐渐减小。

理论 Odin Token 供应量为 $S(t)=4M+p(t)*M*t=M(4+p(t)*t)$ ，又计为 $S(t)=S(t-1)+\Delta S$ ，其中 $\Delta S=p(t)*M$ 。在此基础上，每年广告商都会从代理商那里购买一定数量的 Odin Token，其中 10% 的 Odin Token 将会被烧毁。为了简化发行模型，不妨假设每年烧毁的 Odin Token 数量占当年 Odin Token 总量的比例为固定值 q ，那么最终总的流通中的 Odin Token 供应量会稳定在一个等于年 Odin Token 发行量除以烧毁率的值上。各年度实际 Odin Token 供应量为：

$Sr(t)=(Sr(t-1)+\Delta S)*(1-q)$ ，流通总量趋近于 $p(t)*M/q$ 。下表详细列出了各年度 Odin Token 供应量和烧毁量。

表 5.1 ODIN 供应量和烧毁量

年度	实际 Odin Token 供应量	理论 Odin Token 供应量	Odin Token 烧毁量
0（上线期）	4M	4M	0
1	$Sr(1)=S(1)-S(1)*q$	$S(1)$	$S(1)*q$
2	$Sr(2)=S(2)-S(1)*q-(S(2)-S(1)*q)*q$	$S(2)-S(1)*q$	$(S(2)-S(1)*q)*q$
t	$Sr(t)=(Sr(t-1)+\Delta S)*(1-q)$	$Sr(t-1)+\Delta S$	$(Sr(t-1)+\Delta S)*q$

预定方案决定 Odin Token 供应总量不超过 15,000,000,000，其中 20%分配给早期投资人，20%由团队持有，5%分配给社群和商务合作伙伴，剩余 55%由挖矿产生。为了确保 50 年内理论 Odin Token 供应量和 Odin 系统的整个生命周期内实际 Odin Token 供应量不超过 15,000,000,000，算出增长系数参数 $p_0 = 1.49$ ， $\alpha = 0.83$ ，烧毁系数 $q=0.001$ ， $M \sim 1,687,500,000$ ；当供应量达到 $p(t)*M/q$ 时，每年有 $p(t)*M$ 被挖出，同时有 $p(t)*M$ 丢失，达到一个均衡，如下图所示。

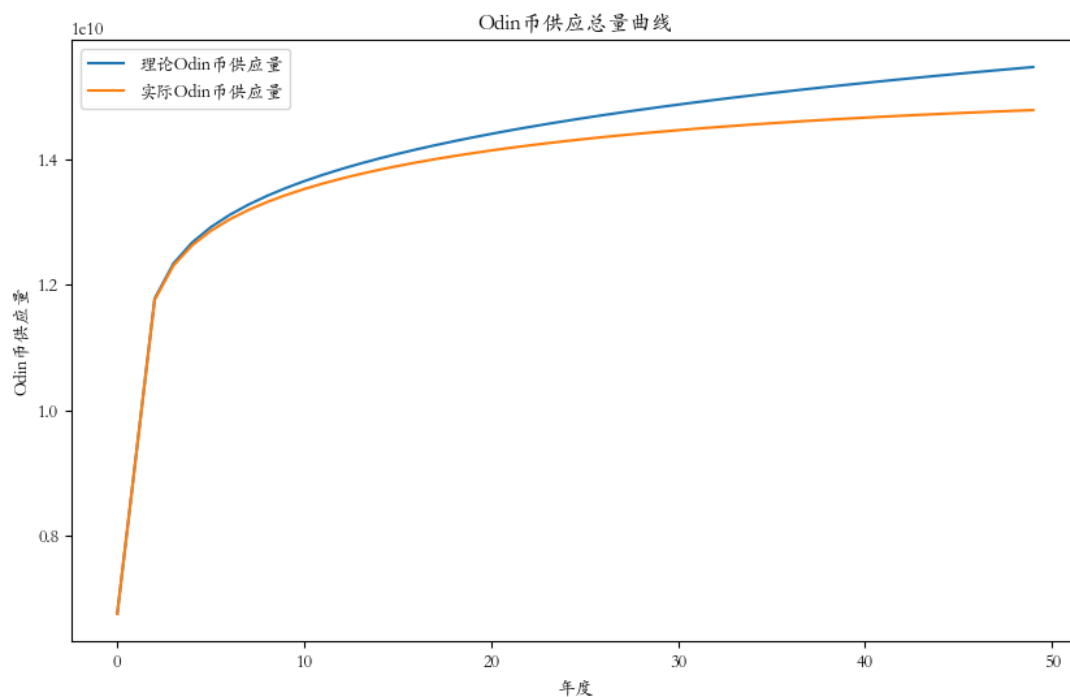


图 5.1 理想和实际的 Odin Token 增长曲线

Odin Token 增长系数变化图如下：

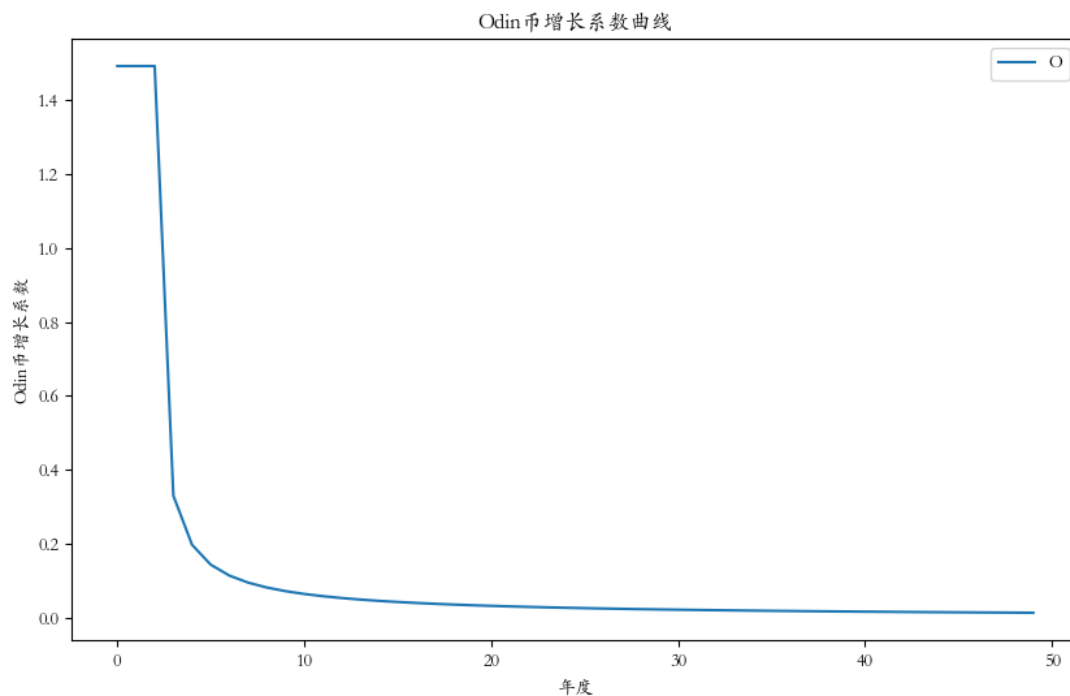


图 5.2 Odin Token 增长系数曲线

非线性增长模型从长期来看“Odin Token 供应增长率曲线”是趋于零的，如下图所示。

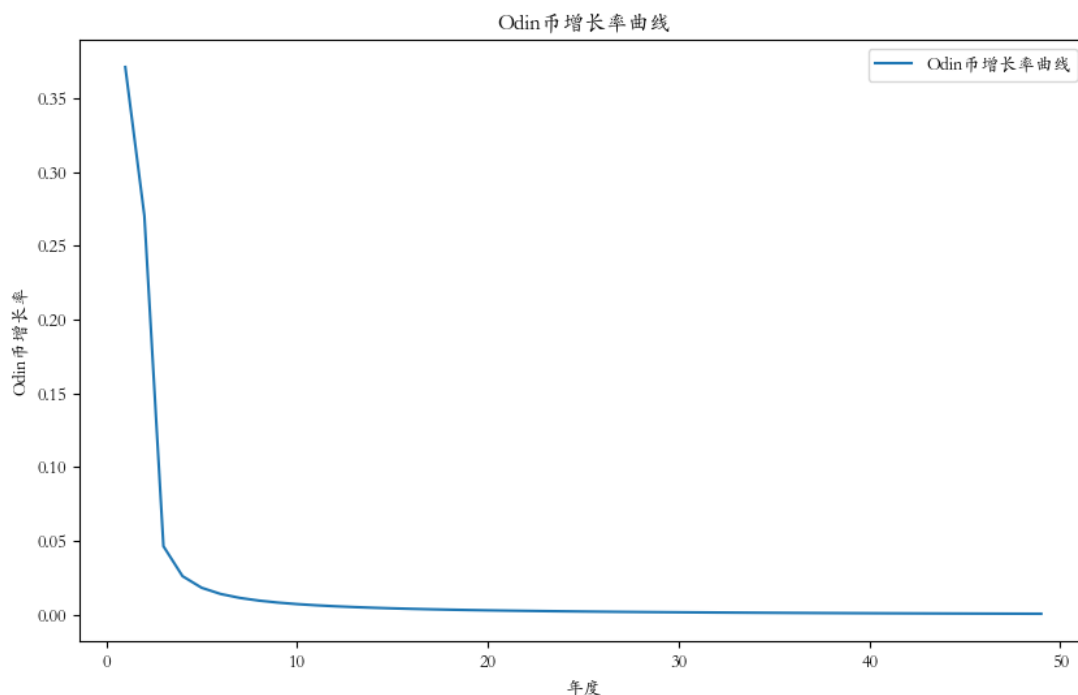


图 5.3 Odin Token 供应增长率曲线

5.3.2. Odin Token 单位

Odin 单位包括：Odin，mOdin， μ Odin；它们的数量关系如下：

$$1\text{Odin}=1000\text{mOdin}=1000000\mu\text{Odin}$$

5.3.3. 难度

每个周期 Odin 系统自动设定一个贡献度阈值，贡献度超过阈值的节点获得记账授权。为了使每个周期获得记账授权的节点比例维持在一定水平上，系统将根据上个周期拥有记账授权的节点比例来调整当前周期的贡献度阈值。定义贡献度阈值为挖矿难度。

Odin 的区块平均每 t 分钟生成一个，这是 Odin Token 发行速率和交易确认速度的基础。不仅是在短期内，而且是在几十年内它都必须要保持恒定。在此期间，计算机性能将飞速提升。此外，参与挖矿的人和计算机也会不断变化。为了能让新区块保持 t 分钟一个的产生速率，挖矿的难度必须根据这些变化进行调整。事实上，难度是一个动态的参数，会定期调整

以达到每 t 分钟一个新区块的目标。简单地说，难度被设定在，无论挖矿能力如何，新区块产生速率都保持在 t 分钟一个。

5.3.4. Odin Token 生成

每个周期内各用户端不断产生贡献度数据，并共识到各个节点的内存中，等到周期结束时记账节点开始计算各用户的贡献度，并根据贡献度给用户发放奖励。奖励以交易的形式被记账节点打包到新区块中。新区块创建后被记账节点广播到全网的区块链节点，进行贡献度证明校验，区块内交易校验；如果校验通过，区块链节点将在本地的区块链末尾添加新交易区块。

此外，Odin 用户之间也会产生 Token 交易，这些交易由记账节点打包到区块中，并经全网共识添加到区块链中。记账节点获得挖矿奖励，奖励以交易的形式发放。

5.3.5. Odin Token 交易的生命周期

一笔 Odin Token 交易的生命周期起始于它被创建的那一刻，也就是诞生。随后，Odin Token 交易会被一个或者多个签名加密，这些签名标志着对该交易指向的 Odin Token 资金的使用许可。接下来，Odin Token 交易被广播到 Odin Token 网络中。在 Odin Token 网络中，每一个 Odin 节点（Odin Token 交易参与者）都被验证，其交易将在网络中进行广播，直到这笔交易被网络中大多数节点接收。最终，Odin Token 交易被一个记账节点验证，并被添加到区块链上一个记录着许多 Odin Token 交易的区块中。

一笔 Odin Token 交易一旦被记录到区块链上并被足够多的后续区块确认，便成为 Odin Token 总账簿的一部分，并被所有 Odin Token 交易参与者认可为有效交易。于是，被这笔交易分配到一个新所有者名下的 Odin Token 可以在新的交易中被使用——这使得所有权链得以延伸且再次开启一个新的 Odin Token 交易生命周期。

5.4. 分配机制

分配模型如下：

- 1) Odin Token 将以每 Odin x 的价格发售给投资者。假设此方式售出 1.777M

Odin。

2) 1.777M Odin 将依照时间锁定合约分配给创业团队，5 年内每年解锁 0.355M。

3) 每年将有 $p(t)*M$ 个 Odin 将被系统维护节点挖出，并分配一定数量 Odin 给 Odin 轻节点。

表 5.2 ODIN 的分配模型

	1 年后	5 年后
Odin Token 单位	5.485M	7.62M
投资者	1.777M	1.777M
创业团队	1.777M	1.777M
社群和商务合作伙伴	0.446M	0.446M
系统维护节点、贡献者	1.485M	3.62M

非线性通胀模型降低了在 Odin Token 那里看到的财富过度集中的风险，并且给予了生活在现在和将来的个人公平的获取财富的机会，同时能够激励人们获取和持有 Odin Token，因为从长远来看，通胀率依然是趋近于零的。此外，大部分参与者对于 Odin 系统的兴趣是中期的。我们预测如果 Odin 成功，则它在 1-10 年的时间段内会经历巨大的增长，而在这期间它的供应量是非常有限的。

6. 团队成员

王鸣（王艳昭）：Odin Chain 的创始人和 CEO。西安交通大学连续创业者，多听 FM 联合创始人，PGYER 联合创始人，天使投资人，雷鸣资本创始人。

王龙：Odin Chain 的创始团队成员。西安交通大学本科和 AI 硕士，美国伯克利大学硕士，安全领域专家，资深创业投资家。

杨虎：Odin Chain 的算法顾问。中国人民大学统计学博士，国防科技大学计算机学院软件工程硕士，丹麦奥胡斯大学访问学者，现任中央财经大学副教授。研究方向为：信息经济、分步式计算、大数据与统计计算、数据挖掘。曾在国内外知名期刊发表多项学术成果，目前承担了国家自然科学基金青年基金、农业部信息中心等单位的多项科研项目，有丰富的科研经验和项目经验。

宋秉华：Odin Chain 的 CTO。中科院网络安全博士，人工智能硕士，IBM 高级系统架构师，东软集团软件架构新技术国家重点实验室高级架构师，大数据专家，在分布式计算、并行处理、图像识别、语言识别、自然语言理解、深度学习、数据挖掘等技术领域有深入的理论研究和丰富的实践经验。在电信、电商、金融、军工、航天等业务领域有丰富的大数据开发经验。

严明辉：Odin Chain 的 CMO。区块链投资人，辉客资本联合创始人，主要投资案例：HLC、MCMCC、火讯财经；项目领域：物联网、媒体、大数据，主要围绕区块链项目生态布局进行早期天使或股权投资，辉客资本合伙人，同时与多项区块链项目投资部保持战略合作关系，围绕区块链生态领域对有助于项目应用和可持续发展的资源进行财务或生态投资建设。

Allen Lee：Odin Chain 的副总裁。QLC 的 Chain Founder 和架构师，十多年的无线网络通信经验，现在 Allen 构建下一代基于 DAG 的网络公链支持去中心化的 NAAS 应用。包括安全网络传输、计费、防火墙和内容感知。在全球最大的通信设备公司工作七年后，带领团队创业开发出 vSIM 系统，4 年时间为 4 百万全球用户提供跨境通信服务，同时 Allen 带领公司完成 B 轮融资。

王多多：Odin Chain 的实验室科学家。西安电子科技大学、西安交通大学 MBA，多个互联网项目的创始人，10 年+工作经验，多年企业应用及移动互联网研发经验。

武雪飞：Odin Chain 的核心工程师。Fog Link OS 操作系统创始人之一，Fota 技术高级架构师，担任掌阅科技阅读及中间件技术架构师（CTO）；千橡互动移动事业部高级工程师；武先生也是 ODIN 的主链构架师，星际区块实验室的 CTO。

7. 进度计划

第一阶段：Odin 链项目立项：于 2018 年 1 月完成项目立项，于 2018 年 5 月发布 Odin 浏览器白皮书。

第二阶段：Odin 链设计开发：将于 2018 年 6 月启动项目设计工作，预计于 2018 年 12 月完成项目开发工作。

第三阶段：Odin 链测试：将于 2019 年 1 月开始内测。

第四阶段：Odin 链公测与上市：将于 2019 年 3 月完成公测后发布 Odin 浏览器产品，并上市。

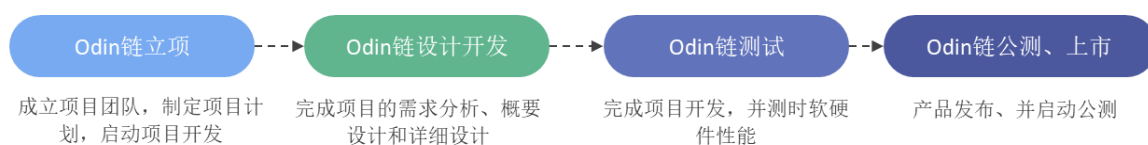


图 22 ODIN 项目进度计划

8. 参考资料

- Aksu, Hidayet, Leonardo Babun, Mauro Conti, Gabriele Tolomei, and A. Selcuk Uluagac. 2018. "Advertising in the IoT Era: Vision and Challenges." *IEEE Communications Magazine* no. PP (99).
- Chen, Lin, Lei Xu, Nolan Shah, Zhimin Gao, Yang Lu, and Weidong Shi. 2017. "On Security Analysis of Proof-of-Elapsed-Time (PoET)."
- Coello, C. A. C., G. T. Pulido, and M. S. Lechuga. 2007. "Handling multiple objectives with particle swarm optimization." *IEEE Transactions on Evolutionary Computation* no. 8 (3):256-279.
- Coker, George, Joshua Guttman, Peter Loscocco, Amy Herzog, Jonathan Millen, Brian O'Hanlon, John Ramsdell, Ariel Segall, Justin Sheehy, and Brian Sniffen. 2011. "Principles of remote attestation." *International Journal of Information Security* no. 10 (2):63-81.
- Eyal, Ittay. 2015. "The Miner's Dilemma." *IEEE Symposium on Security and Privacy*:89-103.
- Eyal, Ittay, and Emin Gun Sirer. 2013. "Majority is not Enough: Bitcoin Mining is Vulnerable." *financial cryptography*:436-454.
- Garay, Juan A, Aggelos Kiayias, and Nikos Leonardos. 2015. *The Bitcoin Backbone Protocol: Analysis and Applications* *. Paper read at theory and application of cryptographic techniques.
- Goldreich, Oded, and Hugo Krawczyk. 1990. "On the composition of zero-knowledge proof systems." *Siam Journal on Computing* no. 25 (1):268-282.
- Goldreich, Oded, Silvio Micali, and Avi Wigderson. 1991. "Proofs that yield nothing but their validity or all languages in NP have zero-knowledge proof systems." *Journal of the Acm* no. 38 (3):690-728.
- Guilford, J. P. 2011. "Varieties of divergent production." *Journal of Creative Behavior* no. 18 (1):1-10.
- Houy, Nicolas. 2014. "It Will Cost You Nothing to 'Kill' a Proof-of-Stake Crypto-Currency." *Social Science Electronic Publishing* no. 34 (2).
- Miralles-Pechuán, Luis, Dafne Rosso, Fernando Jiménez, and Jose M. García. 2016. "A methodology based on Deep Learning for advert value calculation in CPM, CPC and CPA networks." *Soft Computing* no. 21 (3):1-15.

-
- Nakamoto, Satoshi. 2008. "Bitcoin: A peer-to-peer electronic cash system." Consulted.
- Nayak, Kartik, Srijan Kumar, Andrew J Miller, and Elaine Shi. 2016. Stubborn Mining: Generalizing Selfish Mining and Combining with an Eclipse Attack. Paper read at IEEE Symposium on Security and Privacy.
- Qin, L. 2002. Search and Replication in Unstructured Peer-to-Peer Network. Paper read at ICS.
- Roldán-García, María Del Mar, José García-Nieto, and José F. Aldana-Montes. 2017. "Enhancing Semantic Consistency in Anti-Fraud Rule-Based Expert Systems." Expert Systems with Applications no. 90.
- Smyth, Ben, Mark D. Ryan, and Liqun Chen. 2015. "Formal analysis of privacy in Direct Anonymous Attestation schemes ☆." Science of Computer Programming no. 111:300-317.
- Venter, Gerhard, and Jaroslaw Sobieszczanskisobieski. 2002. "Particle Swarm Optimization." Aiaa Journal no. 41 (8):129-132.
- Xing, Bin Cedric, Mark Shanahan, and Rebekah Leslie-Hurd. 2016. Intel®; Software Guard Extensions (Intel®; SGX) Software Support for Dynamic Memory Allocation inside an Enclave. Paper read at Hardware and Architectural Support for Security and Privacy.
- 袁勇, and 王飞跃. 2016. "区块链技术发展现状与展望." 自动化学报 no. 42 (4):481-494.
- Azure, M. Blockchain as a service. <https://azure.microsoft.com/en-us/solutions/blockchain/,2016>.
- Wood G. Ethereum: a secure decentralised generalised transaction ledger, Ethereum Project Yellow Paper (2014) 1-32.
- Cachin, C. Architecture of the Hyperledger blockchain fabric. In Workshop on Distributed Cryptocurrencies and Consensus Ledgers (2016).
- Ross, R., AND Sewell, J. Foldingcoin white paper. https://web.archive.org/web/2016_1022232226/, <http://foldingcoin.net/the-coin/white-paper/>, 2015
- Matchcraft 2016. <https://www.matchcraft.com/how-google-facebook-are-dominating-online-mobile-advertising/>
- Emarketer 2015. <https://www.emarketer.com/Article/Total-Media-Ad-Spending-Growth-Slows-Worldwide/1012981>
- Statista 2015. <https://www.statista.com/topics/2464/yahoo/>.
-