用户至上 可信广告

为广告行业打造的开源协议

白皮书

版本 2021-02-01

目录

术语表

广告预算 指**广告方**为经过验证的**广告声明**所支付的**竞价**总额。

广告购买信息 指的是**广告方**在分形协议中发布的信息，包括目标受众、广告方愿意付费的指定广告行为及针对该行为的出价。一则**购买信息**包括以下指标：**指定动作、用户特征、竞价和广告预算。**

广告声明 **广告声明**会展示**用户**执行过的**指定动作**， 该声明会经过验证者的验证。

广告保证金 指**广告方**要将一部分**广告预算**作为保证金。

广 告 交 易 所 在广告交易所中，广告方和发行方能够进行匹配，发现最优价格，多数交易所都有实时竞价广告拍卖，用户访问发行方网站后，会根据印象调整价格。

广告印象 **指**广告单位的展示及报告。

广告网络平台 该平台集合了发行方的库存供给信息，让供需对接。"广告交易所"逐渐取代了这一术语。

广告市场 指在线广告市场。

广告请求 指发行方向各广告交易所发送的应用程序接口调用，其中包含可售的库存信息以及目前网站用户访问量。

广告标签 指发行方加入网页中的部分代码，用于展示剩余库存类别，供需匹配后，会渲染广告单位，产生广告印象。

广告单位 指经过渲染的广告，例如标语横幅图片、插屏视频和全屏广告。

广告方	通常指的是在线广告推广生态系统中的买方。在分形协议中，**广告方**通过发出**广告请求**，从而让广告接触到目标**用户**。
仲裁保证金	**仲裁保证金**等于**竞价**，在**承保人**提供流动性的情况下，**验证者**如果要验证**广告声明**，需要提供仲裁保证金。
证明者（Attester）	分形协议的参与方之一，负责验证用户**数据声明**，发行**凭证**。
竞价	指**广告方**愿意为经过验证的**广告声明**所支付的价格，是**广告请求**的指标之一。
凭证	由**证明者**发行，用于证明**用户数据声明**的有效性。
需求侧平台	通过平台，广告方能够管理广告活动，从广告交易所及其他库存信息整合方购买广告。
数据声明	该声明由**用户**发送给**证明者**，证明其数据的真实性。
数据管理平台	该平台能够储存和管理信息，与需求侧或供给侧平台相结合，前者提供广告购买信息，后者能放大广告请求，也能展示发行方所掌握的网络用户信息。
FCL	分形协议原生代币
承保方	是分形协议的参与方之一，为验证者提供流动性，支付**仲裁保证金**。
发行方	为广告方提供其网站或者应用的广告容量信息

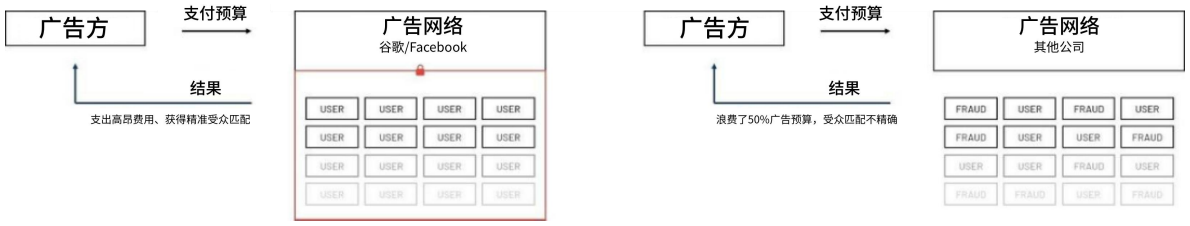
[1] https://www.adjust.com/glossary/advertiser/
[2] https://www.adjust.com/glossary/publisher/

协议	**本白皮书中指的是分形协议**
指定动作	在分形协议中，**指定动作**指广告收费模式，如按展示付费或按行为付费，是**广告请求**的指标之一。
供给侧平台	发行方通过该平台能够管理广告容量信息，改善其网页或应用，以供广告方使用，这一过程最多发生在各广告交易所的实时竞价中
用户	通常指互联网服务的用户，在分型协议中，**用户**通过浏览器插件和数据钱包的技术功能进行交互，发现**广告方**的广告后，会在协议中发出**广告声明和数据声明**。
用户特征	是**广告请求**的指标之一，**用户**只有具备一定特征，才能够满足需求，让**广告方**为**指定动作**付费。
验证者（Verifier）	是分形协议的参与方之一，通过支付**仲裁保证金**，验证用户通过插件和数据钱包发布的**广告声明**。

概要

本白皮书介绍了分形协议，这是一个开源协议，旨在取代广告cookie，让互联网用户重新控制自己的数据。我们希望创建一个数据共享机制，促进公平竞争，打破对价值用户和可信广告的市场双头垄断。该协议创造了动态市场以及技术基础设施，提供激励，让广告市场的价值能够得到更公平的分配。

1. 在线广告生态系统



1.1. 在线广告业 - 免费互联网的支柱

互联网发展的近30年里，在线广告仍然是内容创造者和发行方最可行的盈利策略。虽然通过订阅模式，一些最强大的全球品牌和越来越多抓住商机的发行方取得了一些成功，但总体而言，并没有其他可供选择的互联网广告盈利模式[3]。

在线广告仍然为网络上大多数内容创作提供主要资金。所以，我们认为，要想解决现有问题，最佳方法不是取消在线广告投放（**详见下文第1.2.2节**）。我们更倾向于为内容创造者保留盈利机会，让互联网保持免费和开放，同时调整广告市场中各种激励，达到更好的均衡。

1.2. 广告市场现状

1.2.1. 概况

广告市场依赖于精准定位浏览网页的潜在消费者。而精准定位依赖于对用户准确信息的积累。这让用户数据在互联网中成为一种有价值的商品。

在目前的广告市场结构中，获取用户数据主要有两种途径：

[3] 例如小额打赏等盈利模式逐渐失去优势，因为我们发现用户更喜欢"无障碍"式消费。

1. 跟踪用户使用互联网的全部行为。由于无法知道用户确切身份，观察数据只能够推断出人口特征（例如，用户选择访问的网站或选择购买的东西）。
2. 通过免费互联网产品。谷歌和Facebook[4]一共占了超过60%的数字广告市场份额，占据数字广告行业主导地位，这些广告巨头提供各种各样免费互联网产品，收集用户数据，能够更精准地得出最大规模人口特征。

然后，收集到的用户数据会用于广告市场。在线广告是迄今为止最复杂的数字生态系统之一，尽管如此，我们用简单的语言来描述在线广告的销售和用途。

最常见的情况中，通过各种需求侧平台，发行方通过广告交易所，在实时拍卖中向广告方出售广告空间。

发行方在网站的广告空间中加入广告标签。当用户访问网站时，这些广告标签向广告交易所发送广告请求，提供如横幅大小等广告空间具体参数，并询问价格。广告请求还可以包括发行方掌握的访问站点的用户数据。广告请求中如果包含高质量用户数据，发行方就更有可能以更高价格出售广告空间。这一过程在需求侧平台发生，例如Google Ad Manager或Appnexus。

广告方会调整宣传物料、预算和目标定位等广告活动要素，并通过Media Math等需求侧平台购买广告空间。这些平台能够从各广告交易所和网络（如Google多媒体联播网）获取库存信息。广告交易所联通供给侧和需求侧平台，进行快速实时拍卖，将广告方的广告与发行方的库存相匹配，并确定出售给广告方的广告空间价格。

1.2.2. 广告市场存在的问题

上一节中提到，当前广告市场环境中，用户无法控制自己的数据，导致市场双头垄断，运作效率低下，欺诈行为猖獗。本章节会对这些问题进行分析，以更好理解分形协议在解决这些问题方面发挥的作用。

1.2.2.1. 未经许可收集用户数据

上文提到，用户数据是广告市场中的宝贵资产，对于获取用户数据，最常用的方法是追踪用户使用互联网整个过程的行为。用户浏览网页时，设备中的小型文本文件会记录用户行为，这些文件通常被称为"**cookie**"。cookie有几种类型，但本文会着重强调营销cookie，它会跟踪用户的网上活动，并与其他组织或广告方共享信息。这种cookie的目的是尽可能延长保存时间，换言之，它会一直保留在硬盘中，直到cookie到期被用户或浏览器删除，而且几乎总是由第三方广告商或分析公司投放[5]。

[4] Facebook和谷歌是两个垄断巨头，两家公司在美国、英国和德国的市场总额分别为60.7%、63%和74.5%。详见eMarketer(2019)的"Facebook-谷歌的双头垄断今年不会打破"研究报告，eMarketer(2019)的"2019年德国数字广告支出"研究报告和eMarketer(2019)的"Facebook和谷歌的英国广告市场份额逐渐上升"研究报告。

这种跟踪行为很普遍，往往未经同意[6]而且不透明，虽然一直在减少。营销cookie的减少有很多原因，一方面，隐私监管条例造成了一定的限制，例如，根据《通用数据保护条例》[7]和《电子隐私指令》[8]，在用户不知情且没有获得明确同意情况下，禁止使用营销cookie，所以越来越多人选择禁用cookie；另一方面，如今人们越发对广告表示不满，担心个人隐私，让广告拦截技术逐渐受到欢迎。已经有上千万用户在使用Adblock Plus和uBlock Origin等浏览器扩展程序，而且浏览器本身也让第三方追踪变得更加困难，有些甚至提供了广告拦截功能。

尽管未经许可收集用户数据是一个需要解决的问题，但以上方法本身并没有取得很好的平衡，做到既能保护隐私，又能满足出版方将其内容变现的需求，实际上还强化了广告市场的双头垄断结构，反过来削弱了隐私保护。

1.2.2.2. 双头垄断市场

Google和Facebook两大垄断巨头提供了大量免费产品，一些产品甚至被反垄断机构视为"基本通讯工具"[9]，考虑到这点，这两个巨头非常有可能拥有大量用户访问发行方网站的数据，比如，用户可能使用Chrome作为浏览器，将谷歌搜索作为优先使用的搜索引擎，拥有一个Facebook或Instagram账户等等。谷歌和Facebook的优势在于，它们可以让发行方在竞争出售广告空间时，利用这些巨头掌握的数据。对于访问网站的用户，数据质量和数量越高，发行方广告空间出售价格可能就越高。

第三方营销cookie数量不断减少，阻碍了其他广告网络对用户数据的访问。除此之外，谷歌和Facebook也形成了用户数据孤岛，因为它们的商业模式依赖于这些数据集的排他性。这些因素进一步让数据访问中心化，强化了市场双寡头结构。

---

[5] https://gdpr.eu/cookies/

[6] 虽然通用数据保护条例要求追踪用户数据需要得到明确的同意，但最常见的做法是通过UI骗取用户同意，让大部分用户不知道自己同意泄露哪些信息。

[7] 2016年4月27颁布欧洲议会和理事会条例（EU）2016/679，该条例涉及保护自然人的个人数据处理和这些数据的自耦与移动，废除指令95/46/EC（通用数据保护条例）

[8] 2002年7月12日颁布欧洲议会和理事会指令2002/58/EC，该指令涉及电子通讯行业中个人数据处理以及隐私保护，即 欧洲电子通讯隐私指令。

[9] 2020年，谷歌提起上诉，因为欧盟指控谷歌滥用市场主导地位，为其网络购物币价服务提供优势，HAUSFELD的文章就此事探讨了数字平台能否成为重要通讯设施。

两家垄断巨头产品存在巨大网络效应，让广告市场中的权利更加集中，因为如果你的所有朋友不使用某个社交网络平台，你也不会使用这个平台;一个不是所有人都使用的搜索引擎不会提供最好的搜索结果。对任何公司来说，要想挑战这个双头垄断网络帝国，网络效应是一个进入壁垒。

1.2.2.2.1. 寻租行为

在任何非竞争市场中，如果存在双头垄断结构，除了双头垄断公司，没有其他利益相关者能够获益：

任何非竞争性市场都存在寻租行为，广告市场也不例外。尽管Facebook和谷歌等平台通过自身市场力量，提供更好的广告目标定位，收取更高价格，由于竞争变弱，垄断公司能够利用其市场力量，赚取比在竞争市场[10]更高的价格。这增加了广告方的成本，因为只有少数几种途径才能可靠地接触到用户。

随着发行商越来越依赖第三方数据供应商，主要是Facebook和谷歌，来增加其广告库存的价值，通过广告获得的收入不断下降。出版商也依赖这两家巨头来获得网站和内容的流量，因为登陆他们网站的大量用户是通过谷歌或Facebook等平台[11]。因此，双方议价力量出现不平衡，导致发行方获得的广告收入份额变低。这让发行方越来越不能够产出免费和独立内容，更严重的后果是对整个社会造成损害。下文将会提到，用户本身完全无法参与市场，因为他们不能充分控制自己的数据及其价值。

1.2.2.2.2. 用户产品实用价值有限

除了对自由互联网构成威胁外，广告市场如果存在双头垄断结构，还会对用户产生负面影响，因为用户获得的产品实际效用有限。Facebook等社交网络会产生锁定用户效应，再加上谷歌搜索占了市场份额的 86%，用户转换平台成本非常高，造成了一种不公平的竞争环境，用户并不能真正随意退出平台。因此，用户别无选择，只能同意谷歌和Facebook的强制条款，分享数据，而这些条款并不对用户有利，因为通过这些条款，谷歌和facebook可以利用数字广告

[10] 根据英国公平竞争与市场管理局的网络平台及数字广告业最终市场研究报告，"*在英国，谷歌每次搜索的收益自2011年以来几乎翻了一番，我们比较谷歌和必应的搜索价格，发现在台式电脑和移动设备上，谷歌的搜索价格要高出30%至40%。Facebook的每用户平均收益从2011年少于5英镑增长到2019年超过50英镑，我们通过比较其他社交媒体平台，得知与其他能够获取大量英国用户数据的竞争对手相比，Facebook的每用户平均收益是他们的10倍以上.*"

[11] 市场研究报告第318页

[12] 市场研究报告第319页指出，"就*公开展示渠道购买的广告而言，中介至少能获得35%的利润*"。

[13] 根据Statista《2010年1月到7月全球领先的搜索引擎台式机市场份额》

将这些用户数据变现，却没有给用户足够的回报。无论用户提供的数据多么有价值，这些平台提供给用户的价值只局限在产品的实用价值，甚至在一个非竞争性的市场中，没有足够动力让用户体验到最大实用价值[14].

用户如果使用了广告拦截器，就能有机会保护自己的数据隐私，但这限制了发行方的盈利机会，因此他们只能访问有限内容，要么选择保护数据隐私，要么选择访问内容、使用产品。

1.2.2.3. 诈骗横行，数据质量低，难以归因

广告欺诈横行、数据质量不高导致效率低下，这两个问题非常值得重视。"我花在广告上的钱有一半都浪费了，问题是不知道这些钱都用在了哪里。"这句话非常有力的说明了广告业的现有问题。如今，广告方付费后，互动的主体包括机器人、不相关用户和目标用户，但无法预先辨别以上三者。

在广告业中，各种企业合并正在进行，尽管如此，各大厂商和软件工具有独特的生态系统，这个系统也在不断扩大，限制了互操作性。在这种情况下，广告商很难了解他们的预算在不同广告技术提供商中的分配情况，而后者又是广告方和发行方的中介，技术提供商包括营销机构、归因伙伴、广告交易所、欺诈检测公司、数据管理平台等等[15]。广告技术解决方案变得越发复杂，这让广告商更难有信心地衡量数字广告的表现。74%的广告方表示对数据几乎没有信心[16].

因此，数据缺乏透明度，而这让广告欺诈泛滥[17]。在数字广告支出中，56%的广告呈献给了非目标受众，或者从未真正展示给受众，观看这些广告的是机器人而不是人类。程序化广告欺诈率在10%到30%之间[19]（如果特别针对一场广告活动，这一数字可能高达80%[20]），为了检测欺诈行为，数字广告业已经变成了一场与诈骗者的技术较量，结果是许可欺诈的存在，并将其纳入到产品服务中。

---

[14] 市场研究报告第313页指出，"这种情况正在出现，例如，在Facebook上，每小时平均印象数已从2016年的40-50增加到2019年的50-60。在Instagram上，2019年每小时的印象数为60-70，比2016年增长了200%。这意味着Facebook和Instagram的用户现在看到的广告比以前更多。这些公司想提高消费者对广告的关注，但这会导致用户服务质量下降。"

[15] https://www.iab.com/wp-content/uploads/2016/03/Programmatic-Value-Layers-March-2016-FINALv2.pdf

[16] https://resources.marketingeffectiveness.nielsen.com/blog/keeping-up-digital-advertising-challenges

[17] https://www.emarketer.com/content/digital-ad-fraud-2019

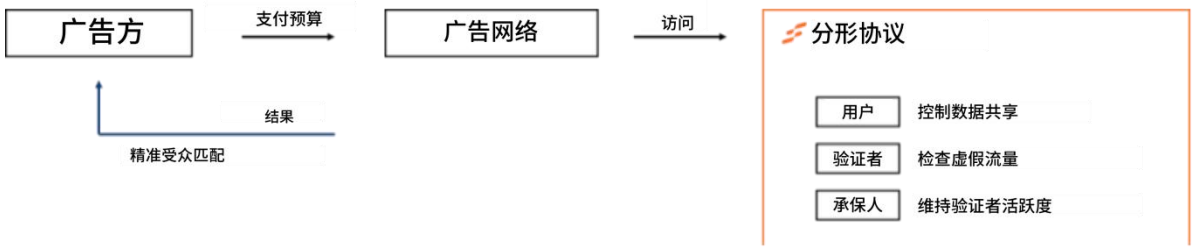
[18] https://resources.marketingeffectiveness.nielsen.com/blog/keeping-up-digital-advertising-challenges

[19] 例如，根据Statista2019年的数据，在澳大利亚，30%程序化广告存在欺诈行为，日本和美国较少，分别是10%和19%。

[20] 行销科技顾问Michael Paxman指出广告预算的80%受到了SDK下载量欺诈的影响。

特别值得注意的是，规模较小的广告商如果不支出昂贵费用，聘请不透明中介，就无法在数字平台之外精准定位目标受众。

2. 数据共享机制案例



前一章提到，尽管数字广告持续增长，但整个行业环境并不能让所有核心利益相关者受益。过去20年里，大量中间商将自己打造成数字广告的推动力量，却使用专有技术，创建封闭生态系统，降低行业透明度，让广告方无法衡量广告表现，从中获利，虽然会让用户反感。

我们认为，只要在协议层面上保护每个利益相关者的根本利益，用户、广告方和发行方之间的利益权衡不会产生问题。用户需要拥有控制数据流的权力，自由地切换不同服务，在共享数据后能得到相应的补偿。广告方需要确保预算能用于创造不受欺诈影响的流量，完成指标。对于发行商，他们需要代理机构的数据，提高库存价值，在机构的控制下，对接库存供需。随着代理机构的增加，整个行业透明度也会提高，最后数字广告生态系统的所有参与者都将受益。

在数字广告业，为了提高均衡度，创造一个新的均衡环境，我们提出在透明的、去信任化的基础设施之上，建立一个广告库存销售和购买激励机制。该激励机制通过区块链技术来实现，保证上述环节执行均可验证，并提供去信任化的公共记录，这样利益相关者在保护隐私同时，也能监控彼此行为，从而减少欺诈。分形协议目的是推动广告市场转型，创造一个开放、公平竞争、没有欺诈的市场。

3. 分形协议 - 数据共享机制

本章会介绍分形协议中的激励系统，以及如何通过该系统解决现有广告市场的低效问题。首先会介绍协议中交互的不同角色，接着对协议中各个环节进行概述。最后，我们总结了这些环节是如何提供激励以推动广告市场的积极转变。

3.1. 分形协议中的角色

分形协议的目标是通过由验证者、承保人和证明者组成的网络，将广告方与用户相连。下面，我们将深入介绍每个角色以及它们如何与协议交互。

3.1.1. 广告方

广告方的目标是传播信息，例如关于产品或服务的信息。他们是广告市场的买方，通过发布广告购买信息与协议交互。广告方信息传达到受众之后才付费，如果发现欺诈，能够得到补偿。

3.1.2. 用户

用户一般指的是浏览互联网的人，就协议而言，用户通过浏览器插件或数据钱包，向验证者提交数据，进行验证，决定是否与验证者共享数据，也会参与到广告方的广告中。

3.1.3. 验证者

验证者连接广告商和用户。发行方、广告网络、广告交易所等都可以成为验证者。验证者通过验证广告声明与协议交互。

3.1.4. 承保方

承保方为协议提供流动性，并能获得质押回报。承保方会根据信誉，向验证者（负责验证用户的广告声明）提供流动性。任何能够提供流动性的人都能成为承保方。

3.1.5. 证明者

证明者通过颁发凭证来验证用户的数据声明，从而与协议进行交互。证明者既可以是身份验证服务提供商，也可以是任何能够确认数据声明真实性的实体.

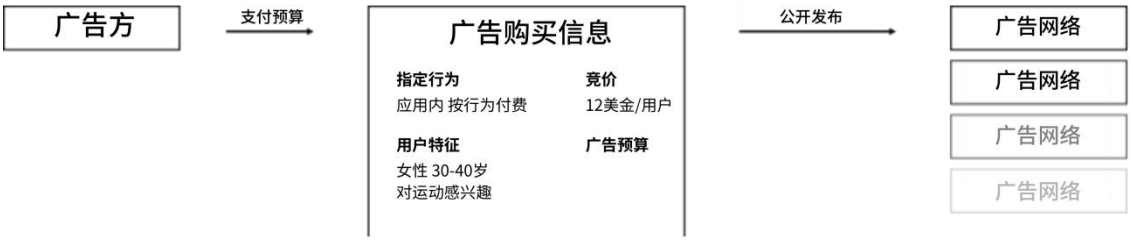
3.2. 分形协议功能

激励机制依赖于协议的一系列功能，这些功能共同提供更高效的市场，促进广告库存的销售和购买。本章节会对这些功能进行介绍和描述。

3.2.1. 发布广告购买信息

广告购买信息由广告方发布，对外展示特定用户动作需求。广告购买信息包括下列指标:

1. **指定动作和动作类型**，例如按展示付费或按行为付费。
2. **用户特征**，例如用户的年龄是30-40岁，或者是合格投资者。
3. **竞价**，例如每个动作收取40USD。
4. **广告预算**，例如总额为4000USD。



以下是对每个广告购买信息指标的详细分析：

3.2.1.1. 指定行为和行为类型

指定动作用于描述广告方希望用户执行的操作。广告方可能想要优化广告活动以取得不同效果，有的要求参与度低，也有的想让用户产生深刻印象。例如，广告方可能想要增加应用程序的用户数量，在这种情况下，他们只想提升应用下载量。他们如果想提升品牌知名度，在这种情况下，会加强广告印象。指定动作按照不同广告模式类别，能分成不同**动作类型**，例如按展示付费、按点击付费，按每次安装付费和按行为付费[21]。各种广告购买信息经过分类会聚集到一起，从而让市场具有可比性（**3.2.6**章节会介绍广告印象市场价格形成）。理想情况下能产生充分形容指定动作的动作类型标准。验证者确认指定动作是否得到执行（详见**3.2.4**章节）。

3.2.1.2. 用户特征

用户特征指广告方的目标受众特征，例如，受众是喜欢狗的葡萄牙人。广告主对其目标受众特征的描述和用户对其自身特征的描述都要遵循同样的标准，这样才能做到精确定位。

3.2.1.3. 竞价

竞价指的是对于每一个指定动作广告方愿意支付价格。竞价金额会分发到验证者、承保人、用户和证明者，因为验证广告声明、维持验证者活跃度、共享数据和向用户发放凭证

[21] CPM即每千人成本。CPA即按行为付费，例如同意一项服务。CPI按安装次数付费。CPC按点击次数付费。

都会得到不同收入。竞价是否得到分配及如何分配不会在协议中公开，目的是为了创造一个高效市场，作为价格发现机制，在这个市场中，利益相关方能对服务自由定价。

通常情况下用FCL来支付竞价，但稳定币会成为主要的支付方式，因为能更好地预测现金流状况，币价保持稳定。分形协议会加入预言机功能，这样兑换价格就能公开到整个网络中。

3.2.1.4. 广告预算

广告预算指的是广告方愿意为竞价支出的总额，FCL可以支付预算，也能作为预算保证金，但是主要支付方式仍会是稳定币，如果要使用预言机功能。

为了发布广告购买信息，广告方必须将一定比例的广告预算作为**广告保证金**。这种机制可以防止网络中出现垃圾信息，让广告方主动删除未被验证者发现的广告，或根据市场调整广告购买信息中的指标，确保支付安全。

广告预算从中心地址中扣除，中心地址用于发布广告购买信息。该地址若没有足够的资金支付竞价，将会在广告保证金中扣除。如果保证金不足，已发布的购买信息将会被取消。

3.2.2. 广告声明和凭证

用户可以共享其特征的证明，协议中的验证者和广告方可以确认此类证明存在且没有被撤销。用户向证明人说明自己某些数据的真实性，即**数据声明**，例如，"我是葡萄牙公民"，并要求后者核实该数据声明是否真实。证明人会根据某些标准，如要求提交葡萄牙公民身份证，执行核实工作。如果确定数据声明是真实的，那么证明人就会向用户颁发一个**"凭证"**。用户能够控制该凭证，例如，凭证会存储在作为数据钱包的浏览器插件中，之后就可以共享给验证者和广告方，同时保护数据隐私。在理想情况下，验证者和广告方能够使用用户数据，但不能访问数据流。凭证发布机制必须能够与广告方描述其目标受众特征的机制进行信息交流，以实现精确匹配。

3.2.3. 广告声明

有了凭证后，用户可以与验证者共享数据。用户登陆一个网站后，验证者提出一个广告请求，该请求包含有用户可能分享的数据，这些数据都经过验证，验证者可以是网站，也可以是运行网站的第三方。

广告请求会给出剩余广告库存及访问网站的用户特征。验证者的广告请求通过相互竞争，获得广告方发布的广告购买信息。验证者如果获得了一个广告购买信息，相关广告单位将向用户展示广告。数据钱包可以证明用户执行了广告购买信息中的指定动作，产生**"广告声明"**。广告声明公开发布后，将等待验证者进行验证（详见**3.2.4节**）。用户生成广告声明，验证者执行验证，这样能够增加透明度，从而更好地监控欺诈行为，例如，用户可能有大量未经验证的广告声明，但与验证者无关，或者验证者有大量造假验证记录，但与用户无关，这两种情况都会存在。

需要注意的是，用户如果没有实际执行指定动作，却发布广告声明，协议中并没有链上机制阻止这种情况发生。所以，验证者会负责验证用户广告声明的真实性。（详见**3.2.4**章节）。

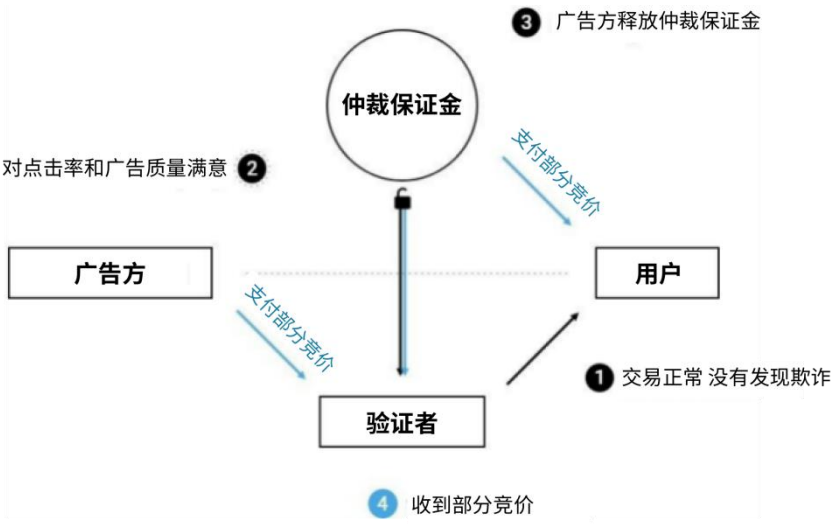
3.2.4. 验证广告声明

验证者可以验证用户的广告声明是否真实。这一过程依赖于链上之外的标志，因此，分形协议并不清楚验证者验证声明真实性依据的标准。为了确认广告声明符合事实，验证者将与竞价数额相等的资金存入**仲裁保证金**。在这个过程中会发生以下两件事：

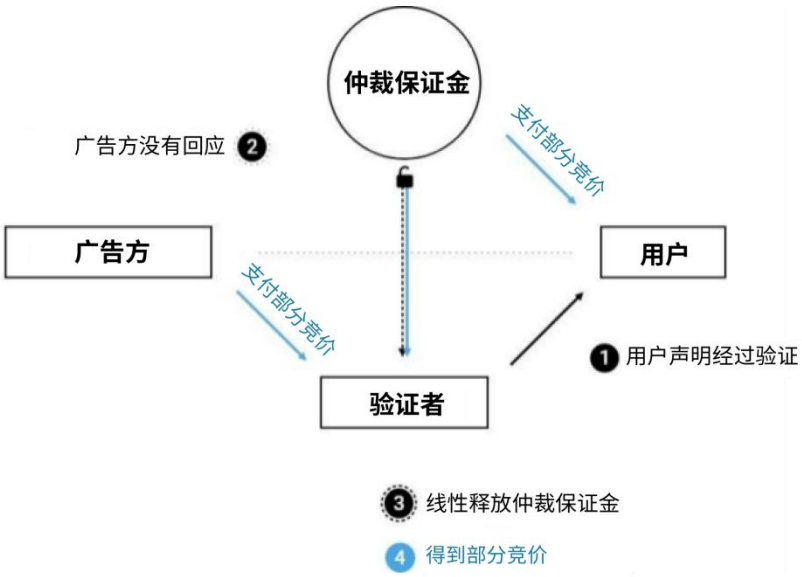
1. 如果要将部分竞价支付给用户，这部分资金[22]从仲裁保证金中扣除，并转到用户钱包中，竞价金额经过一系列分配之后，最终会分配到证明者。
2. 仲裁保证金账户的控制权会转移给广告方。此时可能会出现以下三种情况：

    a) **广告方将保证金归还给验证者**，表明广告方对广告质量满意，成功完成交易，在这种情况下，部分竞价也自动从广告方的中心地址转移到验证者。

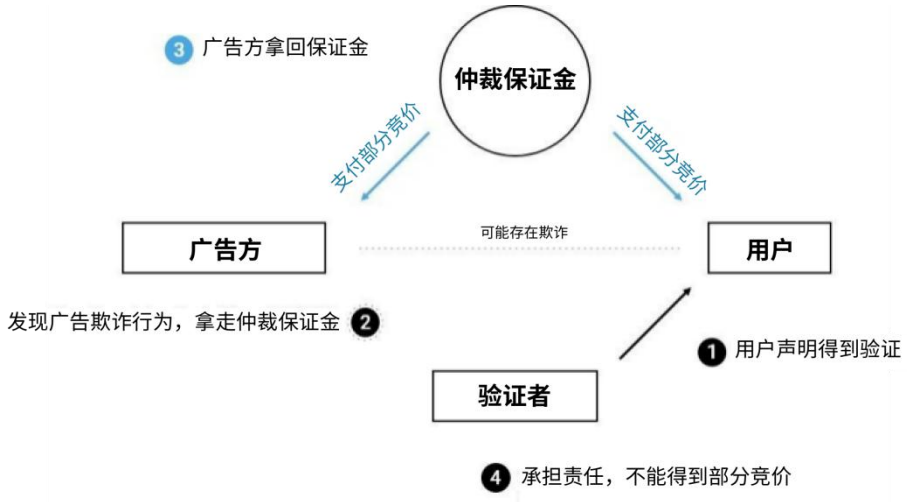
[22] 共享数据后，用户得到的奖励不一定是一部分竞价，奖励也可以是能够访问发行方网站的独家内容。



b) **广告方没有任何回应**，在一段时间后，保证金和部分竞价会线性释放给验证者。



c) **广告主拿走仲裁保证金**，表明广告方不相信广告声明的真实性，认为广告声明不符合验证者的验证，在这种情况下，验证者不会得到自己的保证金（与竞价金额相等）。



无论广告方决定如何操作仲裁保证金，都不会有仲裁过程，因为释放或拿回仲裁保证金只能由广告方作最终决定，不能被逆转。尽管根据协议，若想拿回仲裁保证金，广告方不需要证明验证人存在欺诈行为，因为协议的基础设施保持透明，让广告方尽可能保持诚实，否则，对其他市场参与者而言，该广告方发布的广告购买信息吸引力会降低。

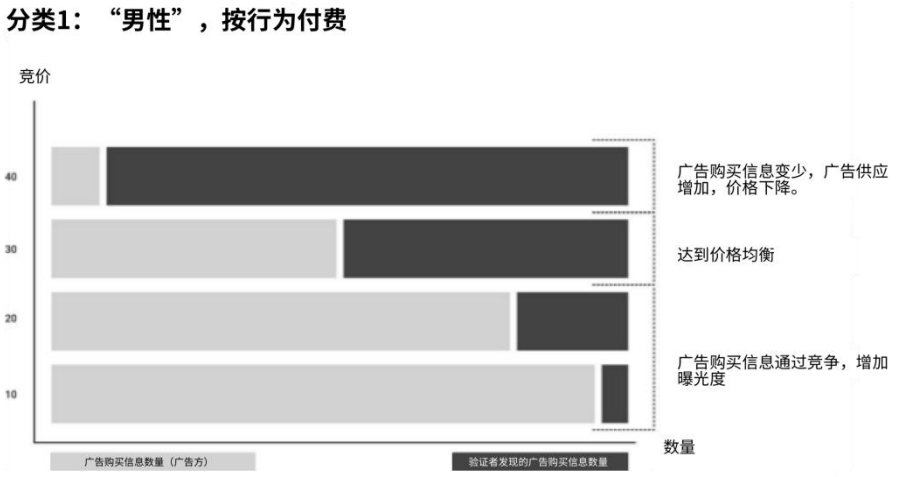
3.2.5. 承保广告声明的验证

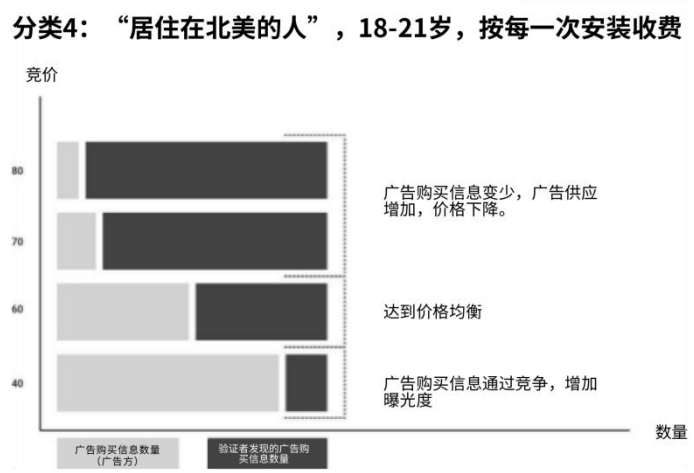
承保人向仲裁保证金提供流动性（**3.2.4**章节详细介绍了仲裁保证金）。任何希望通过在保证金中进行FCL锁仓盈利的人都能成为承保方。

承保人选择一名验证者后，为该验证者质押FCL，当一个广告声明经过验证，且广告方不拿回仲裁保证金，承保人将获得验证者收入的一部分。保费市场会发挥定价发现机制作用，因为承保方的收入会有波动，例如，针对声誉不好的验证者，承保人应向其收取更高的费用。当广告方拿回仲裁保证金时，承保人也会遭受损失。这个过程创造了一个良好市场环境，与存在欺诈行为的验证者相比，诚实验证者能够获得更多流动性。因为在仲裁保证金中，验证者能够拥有的流动性直接与他们验证的广告声明数量挂钩，让更多广告声明得到诚实验证者的验证，减少欺诈行为。

3.2.6. 广告印象市场价格形成机制

广告方的广告购买信息包含指定动作、用户特征和出价，这些要素与验证者的广告请求之间会出现不同组合，推动着广告市场。对指定动作类型和和用户特征而言，这两者的描述如果可以实现标准化，那么针对不同类别，能够形成公平价格发现机制。 例如，根据下图，对于18-21岁的北美用户，在当前的供需情况下，他们每1000个广告印象平均竞价为80欧。





如上图所示，广告印象价格形成机制会影响竞价市场，进而影响用户对验证者的价格容忍度，以及验证者验证用户声明的意愿。核实者愿意用多少收入，换取用户数据，以及用户要求获得多少收入，都将取决于相关类型的市场价格。同样，对于想要获得投资回报的用户，只有他们的数据会得到证明者的证明。

3.3. 均衡的达成

前一节详细介绍了分形协议如何建立一个公开、公平竞争、没有欺诈的广告市场。本章将**1.2.2**节中出现的问题与提到过的解决方案结合，以更深刻理解市场的建立。

3.3.1. 数据主权

如今，广告市场非常依赖于用户数据，通过跟踪用户网上行为收集数据，而这种行为虽然无处不在，但没有经过用户同意，而且不透明，通常情况下，用户几乎不可避免地使用谷歌和Facebook（最主要的平台）产品时提供自己的数据，而且意识不到这个过程的发生[23]。用户无法真正控制收集到的数据，即使他是数据的真正拥有者，只有收集数据的第三方才能将其用于广告市场。

在协议的身份层，用户能够重新控制他们的数据，他们的数据不会被第三方收集和盗用。用户可以利用由证明者组成的网络，为了奖励，证明者会验证用户数据声明，颁发凭证，用户可以决定是否以及如何与验证者共享凭证.

3.3.2. 竞争

第三方cookie已经消失，Facebook和谷歌形成用户数据孤岛，集中数据访问权，从而巩固在广告市场的双头垄断地位。由于高准入门槛和网络效应，对于这两家公司而言，就算有新公司出现，双头垄断地位也不太可能受到影响。

分形协议希望创建一个数据共享机制，促进良性的竞争，侵蚀寻租双头垄断的利润，这样用户就能享受更多产品实用功能。该协议打破了数据访问的排他性，提供激励，建立基础设施，让用户分享经过验证的数据，而验证者可以利用这些数据来销售广告库存，广告方购买数据时也能信任验证者。广告市场竞争日益激烈，降低了现有双头垄断格局的寻租利润，广告方能够获得更大投资回报率，发行方潜在收入升高，用户通过分享数据也能收益。因此，分形协议创造了更好的平衡，既保护了数据主权，发行方也能将其内容变现，这对独立内容创作和自由互联网的存在至关重要.

3.3.3. 欺诈仲裁和预防

广告市场缺乏透明度，存在低质量数据，广告方不得不为非目标或是虚假流量付费。当广告商支付后如果发现欺诈，为了追讨不合理支付的金额，通常需要与广告网络进行长时间且不透明的谈判。

[23] 市场研究报告的第14和15页指出，“我们收集到的证据也证实了，在同意一项网络服务时，很少有消费者阅读隐私政策，例如，在最近的28天中，访问谷歌隐私政策页面平均时间只有47秒，85%的用户时间不到十秒。这样导致了用户只是简单地理解了他们所同意的默认选择。这些选择都是由平台设定的，很难相信平台会照顾用户使用个人数据的偏好，而不顾自身实质性利益”。

分形协议能够标准化目标受众特征的描述，而且标准都拥有互操作性。在协议层面，广告方会根据一定标准来形容目标流量的特征，验证者接受和理解标准。这提高了数据质量，并让广告方能够直观地了解所生成的流量是否符合预期，从而判断支付的款项是否合理。在另一方面，通过仲裁保证金机制，广告方能够分析流量，避免因为错误或是欺诈归因花冤枉钱，付款后也不需要讨论，欺诈验证者将会被排除，因为这些验证者将缺乏承保人的关键支持.

4. 分形协议在应用层的应用

本章节介绍分形协议当前技术方面的应用计划。协议的构建交错进行，通过这种方式，小组件可以自己增加价值，整合到现有广告技术堆栈中。与此同时，我们不断努力构建整个协议，利用从整合中获得的经验，根据新市场状况作出调整。在整个过程中，本章节所述的技术方案将不断改进。

4.1. Web2 组件- 协议用户的交互

在**3.2**章节，我们描述了分形协议的功能，以及参与者如何相互作用，形成一个销售和购买广告的市场。本章节会介绍支持这些交互的web2组件。

4.1.1. 广告方

4.1.1.1. 广告购买信息的发布

广告方将使用我们的web应用程序或API向广告受众展示广告单元。广告方通过web应用程序或API可以做到以下几点：

1. 上传相关广告物料，例如图片、视频；
2. 创建广告购买信息并设置指标（详见**3.2.1**章节）；
3. 在广告保证金中支付部分广告预算。

4.1.1.2. 释放/ 拿回仲裁保证金

广告方通过我们的web应用程序或API，可以查看广告声明，分析验证者对广告声明的验证。基于分析结果，他们可以操作仲裁保证金，释放验证者的押金，或发现欺诈后拿回保证金。广告方通过应用程序可以做到以下几点：

1. 分析验证者对广告声明的验证；

2. 验证者的证明如果符合事实，从仲裁保证金中释放押金；
3. 验证者的证明如果存在欺诈，从仲裁保证金中没收押金。

4.1.2. 用户

4.1.2.1. 数据声明的生成与凭证共享

用户将主要通过两种方式与协议交互，第一种直接通过我们的浏览器插件（作为用户的数据钱包），或通过将交互委托给网站所有者（可能是一个验证者或与验证者合作的发行方）。用户通过我们的浏览器插件可以做到以下几点：

1. 主要通过KILT协议，向证明者发出证明请求，储存发出的凭证。（详见**4.3.1**章节）
2. 能够设置偏好，决定凭证共享的内容，例如，只共享位置但不共享姓名；共享年龄段但不共享具体年龄。
3. 设置能够读取凭证的发行方或网站。

4.1.3. 验证者

4.1.3.1. 寻找合适的广告购买信息

验证者会寻找合适的广告购买信息，他们认为这些信息可以吸引用户完成指定动作。验证者使用我们的web应用程序或API来搜寻广告购买信息，然后与发行方合作（验证者本身不是发布者），把信息发送给合适的用户.

4.1.3.2. 验证广告声明

验证者认为用户已经执行了指定动作，想验证用户的广告声明。为此，验证者可以使用我们的web应用程序或API。这可以帮助他们以下几点：

1. 验证用户广告声明的是否符合事实；
2. 在仲裁保证金中存放与竞价相等的押金，担保交易成功。

4.1.4. 承保方

4.1.4.1. 向验证者提供流动性

承保人信任某个验证者的验证工作，并希望为其仲裁保证金提供流动性。为此，承保人可以使用我们的web应用程序或API。这可以帮助他们实现以下几点：

1. 了解验证者的声誉和表现；
2. 提升仲裁保证金的流动性，支持验证者，帮助他们提升声誉和验证数量；
3. 获得收入。

4.2. Web3组件-安全性、扩展性及可操作性

我们拥有那样的技术。
— 《无敌金刚》开场白

我们想要在Polkadot上构建分形协议。在本章中，就协议的应用而言，我们会介绍Polkadot能够带来的优势，证明我们的选择是正确的。

Polkadot能够提供合适的工具和基础设施，推动协议的成功开发和部署，而在其他平台上，我们要做出妥协。

Polkadot的目标是建立一个多链的生态，每个区块链都会针对特定目的[24]。为了实现这一目标，Polkadot构建了Substrate和基础设施，连接这些独特的区块链，并提供安全保护[25]，Substrate则是软件工具开发包，用于创建与Polkadot兼容的区块链。

平行链基于Substrate开发而成，有各自运行时逻辑。中继链可以为平行链提供安全性和跨链消息传递[26]。一个区块链如果基于Substrate进行开发，更多控制权可以下放到更底层，手续费结构和货币政策也能拥有更多灵活性。另外，基于Substrate开发的链也可以作为平行线程[27]连接到中继链，与平行链相似，但不能很好地保证区块的执行和市场定价。平行链和平行线程都是即付即用。

作为平行链的分形协议

[24] https://polkadot.network/PolkaDotPaper.pdf
[25] https://wiki.polkadot.network/docs/en/getting-started
[26] Polkadot的中继链本身是空白的，不支持智能合约。虽然如此，Substrate提供两个支持智能合约功能的模块，允许Wasm和EVM的运行。带有特定用途的平行链通过利用模块，能够实现智能合约功能。Edgeware尽管不能作为平行链接入，但是上线后拥有自己的验证者集合，支持ink!(Wasm)和Solidity(EVM)智能合约语言。Moonbeam接近接近区块生产部署阶段，初步的侧重点是EVM，桥接以太坊，向网络迁移提供支持。
[27] https://wiki.polkadot.network/docs/en/learn-parathreads

4.2.1. 高安全性

通常来说，要解决高交易成本和当前以太坊公共基础设施扩展性问题，唯一方法是创建单独区块链。维护区块链安全并不是一件容易的事，因为需要增加更多验证节点，并持续提供激励，阻挡攻击者。

在Polkadot中，每个中继链都有各自的验证节点，增加整个网络的安全性，连接到中继链的每一个区块链都能够享有这种级别的安全[28]。

4.2.2. 高扩展性及更低的交易费

Polkadot的TPS比目前以太坊的多10000倍，大大提高了扩展性，对于我们的项目，高扩展性是重要要求，因为分形协议会涉及区块链的高频使用。

性能得到大幅提升后，带宽竞争会减少。另外，每个链都能控制自己的交易费用，让每条区块链都能实现扩展。

4.2.3. 互操作性

在Polkadot中，每个区块链的安全性能够得到确保后，开发者就能专注于构建最适合自身使用场景的区块链。区块链连接后，能够共享不同功能[30]。此外，Polkadot目前正在构建桥接基础设施，这样区块链能够与其他不是基于Substrate开发的区块链进行通信，如比特币和以太坊区块链。

值得注意的是，虽然Polkadot的主网已经发布并且上线[31]，但其生态系统仍在开发中。例如，当前网络中还没有平行链功能，因此也不支持智能合约。

4.3. 与Polkadot的结合

我们选择Polkadot的原因之一是其能够提高互操作性，打算充分利用现有和未来的基础设施。

4.3.1. 身份凭证的发放和验证

分形协议的核心在于能够验证数据。对于用户而言，他们能够证明拥有自己数据的凭证，对于验证者和广告方，他们能够确认这些凭证的确存在而且没有被撤销。

[28] https://wiki.polkadot.network/docs/en/learn-security
[29] https://wiki.polkadot.network/docs/en/learn-comparisons#ethereum-1x
[30] https://wiki.polkadot.network/docs/en/learn-crosschain
[31] https://polkadot.js.org/apps/#/explorer

KILT[32] 是基于Substrate的协议，能够发行匿名凭证，这些自主凭证可验证、可撤销。根据当前分型协议的应用计划，分形协议未来会整合到KILT协议中，以发挥上述功能。KILT协议的核心功能大致如下：

加入KILT协议后的用户：

- 向证明人支付费用，获得声明的证明，即凭证
- 将凭证发送给验证人

加入KILT协议后的证明者：

- 证明声明，生成凭证
- 将凭证发送给用户
- 在链上保存凭证哈希

加入KILT协议后的验证者：

- 信任一位证明者
- 从用户中获得凭证
- 验证凭证哈希在链上的存在
- 向用户请求签名，确认凭证所有权

分形协议也会与Dock协议[33]进行融合来实现上述功能。

4.3.2. 稳定币和价格预言

广告预算和竞价以稳定币计价，这样广告方就能预测现金流。这需要一个预言机来生成FCL和稳定币的兑换价格，并进行喂价。Acala网络[34]能够同时提供这两种功能，因为它不仅提供一个价格稳定的aUSD代币，而且还为预言机功能定价。PolkaOracle[35]也能实现这两种功能。

5. FCL代币的功能

我们希望FCL代币作为协议原生加密货币，推动协议中激励机制的运行。FCL代币有以下功能:

1. 广告方能用FCL支付竞价；
2. 广告方能在广告保证金中质押FCL；
3. 验证者能在仲裁保证金中质押FCL；
4. 承保人能在仲裁保证金中质押FCL；
5. 用户能用FCL支付证明人发行凭证的费用；
6. 证明人发行凭证后会获得FCL。

[32] https://www.kilt.io/
[33] https://www.dock.io/
[34] https://acala.network/
[35] https://www.polkaoracle.com/

我们正在探索这样一种可能性，即FCL能否作为激励，推动分形协议的早期应用，例如，用户能拥有机会对经过证明的数据质押FCL。

分形协议的白皮书后续版本会进一步介绍FCL代币，其中包括代币发行、流通和经济建模。

6. 目前问题

6.1. 发行方的加入

为了鼓励更多人使用分形协议，我们要尽可能简化发行方和其他验证者加入协议的流程。发行方即使没有专家知识或大量投资，也能够发出请求，使用用户数据。我们需要进行更多的研究，了解常见需求侧平台和数据管理平台的整合功能，以及如何通过自定义代码来规避这方面的障碍。

6.2. 滥用广告问题

我们需要进一步建模，开发威胁模型。在用户层面，若能马上发现疑似广告滥用，问题似乎很容易解决。如果决定采用收益共享模式，对于反复访问同一发行方网站的用户，发行方收益增加后，用户的收益才会提高。同样，对广告方来说，选择投标频率不会受限制，因为选择对广告请求投标与否不受用户影响.

6.3. 隐私问题

允许和鼓励个人数据共享必须经过非常谨慎考虑。这不仅在法律角度来看是正确的，更重要的是，从道德角度来看也是正确的，因为隐私监管往往会滞后于技术进步.

6.3.1. 用户的隐私保障

用户要感到对自己的数据拥有主权，这是非常重要的一点，例如，在不知情和未取得同意的情况下，用户可以确认任何数据都不会共享，即使是数据钱包的创建者。开放的生态系统尽管有恶意数据钱包泄露信息，但用户可以建立一个列表，其中包括可信、开源及经过审计的数据钱包，从中选取一个即可。另外，我们需要进一步建模，开发一个减少恶意行为的框架.

6.3.2. 过度收集数据和身份暴露问题

过度收集数据是一个比较难解决的问题。用户一旦与验证者共享数据，必须防止验证者存储、泄漏或转售这些数据。

万一发生了这种情况，会造成棘手的问题，万一有人找到数据点之间的联系，就能发现用户身份[36]。

要想减少出现这个问题，我们需要一种更细致的数据共享方法。理想情况下，验证者能使用用户数据，但不能够访问它们。这一点很难实现，需要进一步研究才能解决。值得注意的是，同态加密会是一个很有前景的解决方案。实现数据"最小化"原则的技术也有望解决这个问题。举例来说，假设有这样一个场景，验证者希望知道数据钱包中有护照的用户的年龄范围。一种简单的方法可能是向验证者共享所有护照数据，验证者可以很容易地从护照显示的出生日期推导出年龄范围。不过，更好的选择是使用零知识证明，如zk-SNARK[37]。通过这种技术，用户能够向发行方证明自己确实在某个年龄范围内，同时不会泄露具体生日日期，更不可能暴露护照全部信息。

6.3.3. 分离效应问题

分离效应是一种新出现的现象，会影响某些鼓励数据共享的系统。如果不解决这个问题，就会导致系统参与者被迫违背自己的意愿共享数据。在分离效应的影响下，如果不披露某些数据，这会被认为是保护数据所有者利益的行为[38]。

举个简单的例子，健康保险公司会对吸烟的投保人收取更高保费。在这种情况下，很多人选择提供他们不吸烟的证据，这对那些不提供证据的人来说是个坏消息。如果不吸烟的人不愿意证明自己的不吸烟这一事实，他们的保费会更高，这不是因为产生了任何额外风险，而是因为在不提供证据的情况下，保险公司会把他们当成吸烟人士。

针对不同数据种类设置请求限制能够减轻这一问题。我们不认为这是一个好的解决方案，因为我们希望既能保持数据不可知性，也能最大化协议的灵活性。因此，我们正在探索同态加密[39]和差分隐私[40]等技术解决方案，希望缓解这个问题。

在这方面，贝叶斯网络隐私保护方案[41] 能够起到很大作用，因为能提供了一种机制，向数据集加入噪声点。噪声点数量可以通过证明得出，并且不会显著降低整个数据集的质量。有了这种机制，发行方能继续使用用户选择共享的数据，但不能判断特定用户数据的真实性，同时可以证明数据平均真实水平。

---

[36] https://en.wikipedia.org/wiki/Data_re-identification
[37] https://z.cash/technology/zksnarks/
[38] https://scholar.law.colorado.edu/articles/177/
[39] https://en.wikipedia.org/wiki/Homomorphic_encryption
[40] https://en.wikipedia.org/wiki/Differential_privacy
[41] https://www.springer.com/gp/book/9789811368363 , https://economics.princeton.edu/working-papers/bayesian-privacy/

6.4. 二次营销

没有第三方cookie的情况下，用户与协议交互的数据钱包可能会被用于二次营销。广告方可以选择不让浏览器保存标识符，即使到期也不交出控制权，向浏览器扩展程序发出信息，将该标识符传给发行方。

6.5. 协议治理

我们希望该协议能够成为一个去中心化的网络。然而，通常情况下，作为一个技术项目，协议的初期决策权由分形协议团队、核心开发人员和我们的顾问团队掌握。我们正在建立治理系统的雏形，一旦协议发展成熟，创始团队会脱离治理，该系统就可以得到应用。白皮书的后续版本将详细介绍我们正在探讨的治理系统.

法律声明

本白皮书的作用是介绍我们对分型协议现有的愿景以及未来计划。

这份白皮书不能概括到方方面面，也没有任何合同关系的要素。该白皮书不应被视为构成任何形式的招股书，不能用于招揽投资，不构成任何投资建议，在任何司法管辖区都不应被视为购买任何证券的要约或提议。

为避免产生任何疑问，需要注意的是，分形协议还没有完成开发，尚未生成FCL代币。本白皮书中关于协议和CL代币的任何陈述具有前瞻性，仅仅反映了团队对分形协议和FCL代币功能的设想。任何已知和未知的风险都可能导致最终结果与声明不同.

分形协议团队无意表达投资、金融、法律、税收或任何其他建议，通过本白皮书或分形团队得出的任何结论和建议都不针对任何司法管辖区。

版权信息

信息反馈

任何对分形协议的反馈都有助于协议的发展。欢迎加入分形协议的Telegram社区(https://t.me/fractal_protocol) 或者通过 support@fractal.id联系我们，期待您的真知灼见。