

基于区块链的在线广告投放模型

陆歌皓 李翔宇

(云南大学软件学院 昆明 650091)

摘 要 以互联网广告为代表的数字媒体广告在飞速发展的同时也显示出许多亟需解决的问题,例如,数字广告的过程不透明,反馈数据造假、多级代理导致的效率低下等问题被放大,广告主的海量投资在不明就里的情况下被浪费掉。区块链技术提供了一种去中心化的、可信任的点对点分布式网络解决方案。文中基于区块链、智能合约等技术,尝试构建了具有分布式点对点网络、去中心化、数据不可篡改、交易过程透明且可追溯、共识信任机制等特点的在线广告投放模型,以探索一种新的广告商业生态系统,为广告主和广告从业者提供安全、自由、高效、自动化、智能化的交易市场。结合在线广告过程,阐述了基于区块链的在线广告投放模型的运行过程。最后,展望了方案中涉及的智能合约、商业模式以及与其他成熟技术相融合等可继续深入探究的方向。

关键词 区块链,数字广告,广告数据,商业模型,PBFT

中图法分类号 TP315 **文献标识码** A **DOI** 10.11896/j.issn.1002-137X.2019.04.047

Online Advertising Model via Blockchain

LU Ge-hao LI Xiang-yu

(School of Software, Yunnan University, Kunming 650091, China)

Abstract Although the digital media advertising industry represented by the internet advertising has rapidly developed in recent years, some urgent problems are continuously emerging, such as the opaque process of digital media advertising, falsified feedback data, low efficiency caused by multi-level agency, and advertisers' resources and funds are wasted without knowing statistical response. Blockchain technology provides a possible solution with a decentralized trusted P2P distributed network. Using the technologies such as Blockchain and smart contract, this paper attempted to construct an online advertising model via Blockchain which possesses some extraordinary characteristics like distributed P2P network, decentration, non-repudiation, tamper-resistant, transparency in trades, traceability and trusted consensus mechanism, so as to explore a new advertising commercial ecosystem, thus providing a safe, unconstrained, efficient, automated and intelligent electronic marketplace for advertisers and other advertising practitioners. In the combination of advertising practice and Blockchain technologies, this paper also depicted a complete running process of online advertising model via Blockchain. At last, this paper gave some prospects of smart contracts and business models, as well as further combination with other mature technologies.

Keywords Blockchain, Digital media advertising, Advertisement data, Business model, PBFT

1 引言

由于信息的爆炸式增长和媒体环境的复杂化,互联网广告发展在带来海量用户流量的同时,也使广告行业出现了许多亟需解决的问题。一方面,广告主购买广告服务的流程并不透明,广告的制作、投放以及数据反馈等各阶段都掌握在广告公司手中,出于利益的考虑,广告的点击率和流量可以被人为地篡改和造假。美国著名商人约翰·沃纳梅克(John Wanamaker)提出:“我知道在广告上的投资有一半是无用的,但问题是我不知道是哪一半。”这一至理名言被誉为广告营销界的“哥德巴赫猜想”,准确地阐述了在无有效监管的情况下难

以准确度量广告效果的困境。另一方面,广告活动的代理机制可能导致效率低下。目前的广告活动普遍使用代理制,一般由广告主、广告代理公司和广告媒介等多方共同完成,难以保证在逐层传递中广告主的需求不出现偏差甚至误传,沟通效率远低于直接联系的方式。

世界著名的广告业巨头电通安吉斯集团(Dentsu Aegis Network, DAN)于 2017 年 6 月发布了《广告支出预测报告》^[1]。报告指出,2018 年数字媒体广告全球广告支出份额预计将首次超过电视广告,达到 2158 亿,占比 37.6%,成为广告支出占比第一的媒体类型(具体数据如表 1 所列,其中括号中的数据为 2016 年 9 月发布的预测值)。数字广告支付份

到稿日期:2018-03-20 返修日期:2018-06-29
陆歌皓(1977—),男,博士,副教授,主要研究方向为区块链、人工智能, E-mail:glu@ynu.edu.cn;李翔宇(1994—),男,硕士生,主要研究方向为区块链、共识算法, E-mail:553278390@qq.com(通信作者)。

额的不断扩大进一步说明了解决在线广告业中数据伪造、低效率性等问题的迫切性和重要性。

表 1 2016—2018 年不同媒体所占的全球广告支出份额^[1]
Table 1 Global advertising spending share of different media form
2016 to 2018^[1]

(单位: %)			
媒体类型	2016 年	2017 年	2018 年
电视广告	38.4(41.1)	37.1(40.3)	35.9
报纸广告	10.5(11.0)	9.2(9.9)	8.2
杂志广告	6.3(6.4)	5.9(6.0)	5.6
广播广告	0.5(6.4)	6.3(6.2)	6.1
影院广告	0.6(0.6)	0.6(0.6)	0.6
户外广告	6.2(6.9)	6.2(6.8)	6.1
数字媒体广告	31.5(27.7)	34.8(30.2)	37.6

区块链技术的提出在技术上为解决上述问题提供了机遇。本文提出和设计了一个基于区块链^[2-3]的在线广告投放模型(Online Advertising Model Via Blockchain,OAMVB),尝试解决在线广告投放过程中数据造假、多层代理、效率低下等问题,从而实现一个交易过程透明、可追溯、不可篡改、无中介代理的高效率广告投放流程。该模型具有以下特点:

- 1)多中心化广告联盟区块链(Multicenter Advertising Alliance Blockchain,MAAB)。每一个广告公司作为一个独立节点,而不再是作为代理介入广告活动,共同作为联盟管理者管理广告联盟。
- 2)可关联的区块数据结构。自定义了一套适用于广告投放过程的区块存储结构。在保证区块不可篡改特性的条件下关联相关区块,优化查询效率。
- 3)广告贸易过程、投放过程和反馈过程刻画。广告交易、投放和反馈等过程中的各个重要节点将被记录在区块链上,以保证整个交易过程的准确性,完全杜绝交易过程不透明、交易方抵赖、造假的可能。
- 4)微服务架构^[4]。广告投放将由微服务的方式提供给广告媒体,只需在应用中按需选择并使用微服务 API 即可完成投放,保证整个广告过程灵活、易扩展。

- 5)与场景结合的广告奖励机制。根据应用场景将广告与广告受众的需求相结合,提出了更加有效的广告奖励机制。

本文第 1 节介绍了数字广告行业的发展现状,阐述了广告行业面临的痛点问题,并介绍了 OAMVB 的特点;第 2 节介绍了在线广告投放模式的发展状况以及相关技术;第 3 节详细阐述了 OAMVB 的各环节;第 4 节通过与现有问题和目前已有的解决方案作对比对模型进行评估;最后总结全文并展望未来。

2 相关工作

2.1 在线广告投放模式的发展现状

非区块链在线广告投放模式^[5-6]至今已经非常成熟。广告投放的方式具有多元化、精细化的趋势。广告受众与广告发布不再是单向线性发布,而是借助大数据等技术清晰地勾勒出用户画像,了解受众的基本和根本需求,传播符合受众感兴趣的广告信息,力求达到高效、精准的传播。

目前,已经有数百家在线广告平台在国内外上线运营,著名的有 Google AdWords^[7]、多盟、今日头条等。在线广告平

台的发展也促使了广告交易的生态链发生变化^[8]。例如,广告参与方由传统的三主体(广告主、代理商(广告公司)以及互联网媒体)转变为四主体(营销主、需求方平台(Demand-Side Platform,DSP)、交易平台和互联网媒体),且随着一系列细分平台的出现,广告生态链内出现了越来越多的独立链条。

从广告评估效果方面来看,目前流行的反馈指标仍然是以每千次展示成本付费(Cost Per Mille)作为主要付费方式的,此外还存在其他反馈指标,如每次点击成本(Cost Per Click,CPC)等,但少有平台使用。这些反馈标准因为未考虑广告发布的实际效果,使广告公司易使用成本极低的机器人伪造曝光反馈数据,从而导致广告主每年因虚假曝光度的被骗费用高达 180 亿美金^[9],这也体现出了解决广告数据不透明、数据造假等问题的迫切性。为尝试解决这些问题,我们创新性地提出了基于区块链的在线广告投放模型。

2.2 国内外研究状况

目前,区块链技术在各大领域的研究很多,但在在线广告投放领域中的研究较少。区块链技术的不可篡改、去中心化特性能够从广告交易源头消除广告数据伪造、透明度缺失等问题,因此区块链技术被视作能为广告行业带来革命的关键技术^[10]。位于洛杉矶的广告科技初创公司 MetaX 与区块链软件公司 ConsenSys 共同合作签署了一份协议,并声称该协议是第一份协调数字广告供应链区块链协议,称为 adChain(广告链)^[11],提出了广告主、广告发行商和 adToken 持有人之间的良性激励架构,承诺能够解决在线广告业中的主要问题。来自视频娱乐软件厂商 Stremio 的团队计划在 2018 年 2 月发布基于区块链的广告交易网络平台 adEx(Beta)^[12],帮助广告主、广告媒体和用户建立透明化交易模式。对比发现,相较于国内,国外的实验性项目较多,然而总体上国内外的区块链广告发展仍然处于起步阶段。

2.3 区块链技术

区块链技术^[13-14]最早是指以比特币^[15]为代表的数据虚拟加密货币的核心技术,可以通过数字加密、时间戳、分布式存储、共识机制和经济激励等手段来实现去中心化的网络,保证数据不可篡改和不可抵赖,从而解决中心化机构高成本、低效率、数据安全性不足等问题。如今,区块链技术不仅应用于数字虚拟加密货币体系中,还利用自动化代码(智能合约^[16-17])可在可编程金融系统和其他的可编程商业系统中崭露头角。

2.3.1 PBFT 共识算法

PBFT 算法是为了解决分布式系统中互不信任的节点如何达成共识而设计的,它能够保证在至多 1/3 的节点失效的情况下达成全网一致的共识。其基本思路是利用 3 次全网广播在网络中投票选举出最多人认可的结果。由于 PBFT 算法并非为区块链技术而设计,因此在一些细节上仍然可以进行优化与改进,如垃圾回收机制等。

2.3.2 Merkle Tree

Merkle Tree^[18]是区块链中重要的数据结构之一,其作用是能够快速校验数据在区块中的完整性和存在性,提高区块链各节点对区块数据进行检查校验的效率。以二叉 Merkle Tree 为例,其基本原理是将底层数据库中的完整数据通过哈希运算(Hash Function)^[19]得到的哈希值作为叶子节点,让相

邻叶子节点两两结合计算出新的哈希值作为它们的父节点,如此递归直到父节点唯一,称该唯一的父节点为 Merkle 根(Merkle Root),并记录在区块头中。如果区块内任何一个数据发生改变,数据所对应的 Merkle Tree 分支也会改变,因此只需验证 Merkle 根是否相同即可判断数据是否被篡改,并且在不需要完整检查的条件下可通过被修改的各分支定位到具体的被修改数据。

2.4 微服务架构

微服务架构(Micro Service Architecture,MSA)是一种设计应用服务的新技术,其中心思想是围绕特定功能(如账单管

理),为功能设计出独立的业务逻辑和控制器,使服务可以通过调用 API 的方式灵活应用于其他服务或应用中。微服务可以将复杂的大型系统拆分为众多的小型应用,让不同用户、设备和场景都能选择不同的服务,实现按需取用、精准控制的需要。

3 在线广告投放模型

3.1 概述

在线广告投放模型的主体是一个覆盖在线广告全程的广告服务平台,其主要结构如图 1 所示。

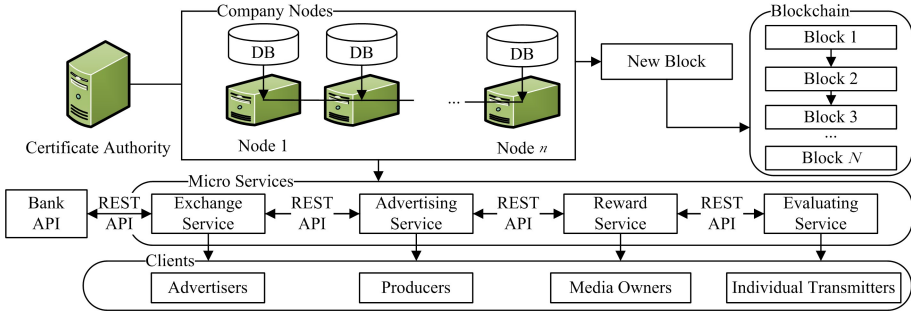


图 1 模型的总体结构图
Fig. 1 Overall architecture of model

根据广告活动的过程将参与广告活动的用户分为 4 类:广告主(Advertisers)、广告制作者(Producers)、媒体拥有者(Media Owners)、个人传播者(Individual Transmitters)。广告主是广告活动的发起人,需要购买广告服务,将信息广而告之;作为广告服务商(Service Provider),广告制作者负责根据广告主的需求生产广告内容、包装广告;而媒体拥有者是拥有传播渠道的广告展示者,负责将广告内容展示给广告受众;除了上述 3 种广告活动的直接参与方,个人传播者是为了获得利润,自愿参加广告传播活动的普通用户。

为了解决数据透明问题,我们提出了使用关键点(Key Point,KP)来记录完整的广告活动。将广告活动细分为多个阶段,每个阶段都具有确定的结果并且各阶段间相互连接,每一个阶段结束后会生成一个关键点,关键点具有以下 3 点特征:

- 1)确定性。关键点能够完全表示一个阶段内的所有确定结果。
- 2)时序性。关键点是下一阶段开启的必要条件,依次按时序排列。
- 3)完整性。所有关键点的集合能够无歧义地完整解释整个广告过程。

OAMVB 并不关心这些阶段的具体过程,而是通过时间限制和奖励机制促使参与方生产关键点,并将关键点存入区块链中。具体来说,广告主与其他服务商签订合同、确权等关键行为都能促使系统生成关键点,这样既能够保证数据准确真实且不可被篡改,也能够极大地节省节点的存储空间。同时,因为参与各方直接与广告主进行沟通,解决了多层代理效率低下的问题。此外,我们设计了可关联的区块存储结构,充分利用关键点的关联性特征,将存储关键点的区块关联起来,优化区块的查询校验效率。

在模型中,广告服务以微服务的形式提供 REST API 和

SDK 给相关服务商,服务商能高效地将广告内容顺利投放到应用中。另外,所有的数据反馈通过平台反馈机制自动监测服务效果,促进服务商提供更好的广告服务,杜绝了人为修改反馈数据的可能。为了保证模型的正常运行,我们设计了奖励机制来保证广告交易各方严格执行模型设计的流程。针对非注册的普通广告受众,需要设置一定的奖励保证广告投放的效果。

最终,整个广告过程以关键点序列的形式完整地记录在区块链中,这一过程被划分为广告交易、广告服务和反馈 3 个阶段,被称作广告过程刻画(Portrayal of Advertising Procedure,PAP)。一次广告过程刻画将与真实的广告活动过程逐一对应,使得数据真实透明。平台还将综合用户个人打分与智能合约的各方履行状况为用户评级,为后续的其他广告交易提供参考,形成完整的闭环,促使参与各方进入良性发展循环。

3.2 基于许可网络的多中心化广告联盟区块链

我们的模型是基于区块链网络构建的,其本质是由多个节点组成的分布式网络,网络中的每个节点都是一个副本,完整存储了所有广告内容和提供的广告服务。通过研究广告活动的特征,发现了以下 4 个要点:

- 1)广告活动需要存储的数据包含大量的音频、图片、视频等多媒体文件,对存储设备的性能和空间的要求较高。
- 2)广告交易各方除了有规模的团体组织,还存在大量的个人用户和小规模团体,网络连接质量、数据处理和存储能力的差异巨大,大多数设备都难以负担存储节点的压力。
- 3)参与各方必须已知身份,且服务商应该有相应的服务资质。
- 4)广告活动内的数据并非完全公开,而是需要具有特定权限才能查看。

基于以上分析,不同于比特币这样的公有区块链,我们设计了基于许可网络^[20]的多中心化广告联盟区块链,所有的参与者都是在身份得到验证后加入到网络中的。区块链主节点也是广告联盟的管理层,最初由不参与广告交易的广告公司担任,这些广告公司也是广告联盟区块链的最初主办方,其主要职责有:

- 1)提供广告投放平台的各项基本服务,保证服务可用。
- 2)共同维护网络稳定,维护网络服务器。
- 3)审核申请者的入网申请和信息修改申请。个人申请者需要提供身份证等必要信息,企业申请者需要提交企业资质和负责人等关键信息。
- 4)审核服务商提交的凭证资料,以保证平台服务被正确部署。
- 5)寻找优质的服务商加入广告联盟。
- 6)共同决策和管理广告联盟,如决定是否添加新节点或删除已有节点等。
- 7)为用户提供资讯和其他有义务提供的帮助。

广告公司最初将通过提供平台服务收取服务费和交易手续费来盈利,随着广告交易量的增多以及数据量的不断扩大,广告公司可以依托庞大、详细的交易数据结合大数据、人工智能等技术推出更丰富、更专业的有偿服务。广告公司参与广告联盟管理,在完成管理责任的同时将产生贡献度(Contribution Degree Point,CDP),贡献度越大其可靠性越高,公司之间将按贡献度决定收益的分成比例,分账合约将被设计成智能合约并由智能合约自动执行。同时。CDP 还将作为共识机制改进的基础,共识机制的改进将在 3.3 节中详细说明。

其他各类普通用户不作为独立节点存储区块链记录,而是通过身份认证的形式注册成为任意一个主节点的成员并且分配独立的私钥,私钥由管理节点共有的 CA 服务器颁发。当普通用户满足一定的条件(如规模、评分等)时,也可以向管理层申请成为存储节点,在承担管理责任的同时也享受相应的权益。网络将优先保护参与方的数据权益,根据广告交易各个阶段的确权过程,所有信息都有确定的所有权,信息拥有者使用自己的私钥对内容进行加密,有权决定是否展示给申请者查看,仅当申请者被允许时,才可通过提供的通道查看相关的信息,满足了参与各方对信息安全的要求。

在广告活动中,普通用户是某一主节点的成员,其提交的请求被分为两类:关键点请求和非关键点请求。关键点请求(见表 2)是指客户端请求在达成全网共识后结果将作为关键点写入区块链的请求。其他的请求并未形成关键点,其数据存储在用户所属节点内,不进入全网共识阶段,为将来可能形成的关键点提供数据支持,如创建合同、合同审核等操作。

表 2 关键点请求
Table 2 Key point requests

Request	Description
所有合同确认请求	合同签订双方确认合同内容并使之生效
所有验收请求	如广告作品验收,服务效果验收等
所有交易请求	如支付货款等操作

关键点请求的具体步骤如图 2 所示,具体描述如下。
步骤 1 用户发送请求给所有节点,包括用户的身份认

- 证信息(如公钥、token 等)。
- 步骤 2 节点各自执行请求并将其存入本地日志中。
- 步骤 3 节点判断请求是否为关键点请求,若是则由用户所属节点返回结果;否则进入步骤 4。
- 步骤 4 节点生成待确认区块,区块进入共识过程,为请求的结果寻求共识。节点通过本地存储的日志与其他节点对比完成验证。
- 步骤 5 已验证区块被写入区块链,媒体文件加密存入分布式数据库。
- 步骤 6 节点各自返回结果给客户端。
- 步骤 7 客户端验证结果后反馈给用户。

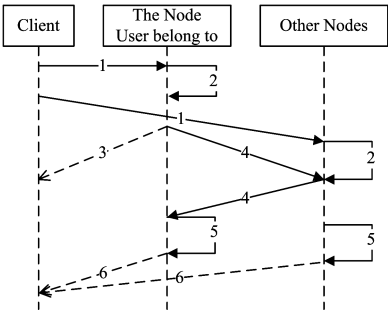


图 2 关键点请求的步骤
Fig. 2 Steps of key point requests

3.3 改进的 PBFT 共识机制

每一个管理节点都是身份已知且经过认证的,各节点之间拥有更高的信任基础,网络节点规模较小,并且广告活动的多样性对交易的确认时间和效率的要求较高。我们使用了 PBFT 状态机复制算法^[21-22],保证在有至多三分之一的节点失效的情况下能够达成共识并保证交易的高效达成。研究发现,PBFT 算法并非专门为区块链网络而设计,因此结合模型特征做出了以下几点改进:

- 1)管理节点的可靠性由贡献值 CDP 表示,在选取 primary 节点时,首先将节点按 CDP 值排序,由 CDP 值高的节点优先担任 primary 节点。PBFT 算法中对所有节点一视同仁,primary 节点由所有节点依次担任。但实际上,管理节点的各公司的可靠性各有不同,可靠性越高的公司其节点就越稳定。因此,在 primary 节点的选取过程中加入对节点 CDP 值的考虑,能够减少主节点失效的可能,从而降低节点切换造成的通信开销,提高整体效率。
- 2)通过区块链实现垃圾回收机制。PBFT 算法通过消息广播的形式传递消息,网络开销极大,除了必要的三段协议外,PBFT 算法提出了垃圾回收机制——检查点协议。该协议的目的是通过一次全网共识来决定是否删除一系列已处理的用户请求,其过程仍然需要一次消息广播,目的是保证垃圾回收机制满足活性和安全性(Liveness&Safety)^[3]。区块链网络中,每一次用户请求结果在全网达成一致后都将被封装成区块保存在区块链中,因此一个生效的区块同样满足活性和安全性。因此,只要设置一个时间阈值,各节点每隔一定时间检索区块链内的区块,并将区块对应的请求日志删除即可完成一次垃圾回收。同时,由于区块链和 PBFT 算法都使用了时间戳,区块和用户请求都是按时间顺序排序的,因此搜索

请求对应的区块也是高效的。

3.4 可关联的区块数据结构

在模型的区块链中,所有信息都存储在区块结构中。由于关键点具有时序性和完整性,一个完整广告活动必须由多个区块顺序串联才能完整表示,而相邻关键点生成的时间间隔可能较大,因此会导致在区块链中同一广告活动的相邻区块间隔较远,影响查询效率。如广告主与广告制作者签订广告制作合同,并与媒体拥有者签订广告发布合同,期间时间间隔为 15 天。在这段时间内,有其他生成的区块加入到区块链中,导致记录两个合同的区块编号相差上千。当需要查找相邻关键点时,需要上千次的对比,并且平台内的广告活动越多,效率问题就会越严重。为解决上述问题,我们设计了针对广告活动特点的区块数据结构——关联区块(Cognate Block, CB)。

关联区块包含两个部分:元数据区和数据区。元数据区记录了该区块相关的元数据信息,如表 3 所列。数据区记录了每个信息的摘要(Abstract)、元数据(Meta-data)以及由信息生成的 Merkle 树(Merkle-tree)。

表 3 元数据结构

Table 3 Structure of meta-data

Field Name	Size/Byte	Description
版本号 (Version)	4	用于区块监测与升级的标识
父块哈希值 (Prev-hash)	32	指向父区块哈希值,定位父区块位置
计数器 (Count)	可变量整数	存储数据份数
Merkle 根 (Merkle-root)	32	存储数据构成的 Merkle 树根的哈希值
关联哈希值 (Cognate-hash)	32	指向同一广告活动的上一相邻区块哈希值
时间戳 (Timestamp)	4	区块生成时间
标签 (Tag)	1	标记区块的身份(如关联区块起始位置等)

信息的元数据包含了该条信息的类型(Type)、拥有者公钥签名(Sign)、时间戳(Timestamp)等。如果原始信息较小(如 IP 地址等),则信息摘要就是信息本身;如果原始信息大于 32 位哈希值长度,则将原始信息存入分布式数据库中,并求得其哈希值作为索引和信息摘要。

关联区块的生成依赖以下两种不同的策略:

1)关键点生成策略。关键点生成策略是在关键点形成时根据关键点的各项信息生成对应关联区块的策略,关键点信息作为信息源计算元数据,如时间戳等。关键点信息的规模一般较小,如一个广告合同生效时请求生成的关键点可能包含合同本身、相关附件等数十项信息,其信息摘要仅占数 kB 到数十 kB 不等。因此,关键点信息生成的管理区块数据区的大小上限设置为 100kB。

2)反馈生成策略。反馈生成策略是在广告服务阶段,系统自动收集广告点击浏览信息,每分钟统计一次或数据区被填满时将广告点击者的 IP 等信息作为数据生成区块链的策略。与虚拟货币交易记录类似,广告点击信息是数量极多的小数据集,如一分钟内可能有数万以上的浏览者点击和浏览平台内的不同广告,因此我们采取成熟的比特币区块大小,将由反馈信息生成的关联区块数据区大小限制为 1 MB。经过粗略计算,若每次广告访问时仅存储访问的 IP 地址数据,

则一分钟内一个区块可存储约 26 万条信息。当每分钟广告访问数据大于区块数据区大小时,系统将生成多个区块以满足访问量记录的需求。

关联区块具有独特的字段:关联哈希值(Cognate-hash)。无论采取何种生成策略,新区块生成后仍然遵循链式结构链接到区块链中的最长链末端,同时会在关联哈希值字段记录相同广告活动的上一个关联区块哈希值,通过“搭桥”的形式将同一广告活动的相关区块联系起来,如图 3 所示。关联区块的起始位置是整个广告活动结束时产生的最后一个区块,由标签(Tag)字段标记。当以关联哈希值为索引溯源时,能够高效地完整遍历该广告活动的所有相关区块。由于区块地址是对完整区块哈希运算后得到的,若篡改其中任意一个块,都需要修改区块链中的其他所有块,因此关联哈希值字段的增加并没有因为缩短了实际遍历的区块数而损害区块链的安全性。

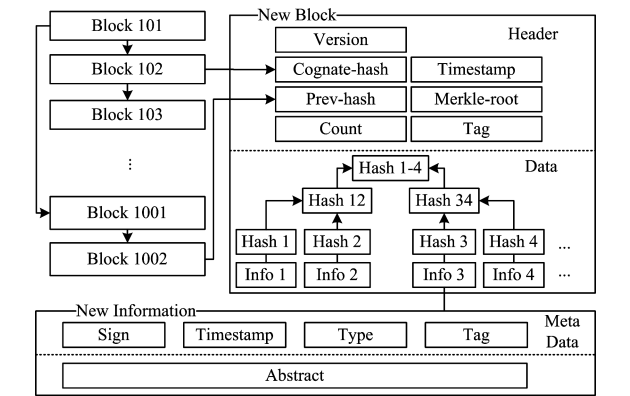


图 3 关联区块的结构

Fig. 3 Structure of cognate block

3.5 广告过程刻画

在广告活动中,各类用户根据角色的不同被分配不同的权限,以及开放不同的功能,以保证每一个角色各司其职,不能干预其他环节的活动。一个服务商可以在交易过程中扮演多种角色,如可同时作为广告制作者和媒体拥有者的广告公司,但每一个角色的认证都需要单独提交审核材料以满足各角色的准入标准。除个人推广者外,其他角色准入条件较为严格,个人申请者需要提供身份证和要求提供的服务资质证明并接受平台的人工查询和验证,非个人申请者还需提交营业执照等具有法律效力的可证明身份和服务资质的材料。个人推广者面向普通网络访客,其仅需要提交身份证、个人银行卡并通过视频认证等方式验证身份真实即可批准入网。个人推广者不参与广告交易,仅能够通过任务发布平台接取推广任务赚取佣金。

准入的所有广告主与服务商将收到由中国金融认证中心(China Financial Certification Authority, CFCA)[23]颁发的认证证书和电子签章,在平台内签订的所有电子合同都将进行签章和证书认证,以使合同具有法律效力。

每种角色在入网审核通过后都需要填写自己使用的银行账户,所有交易发起时买方都需要首先支付预付金或全额货款,平台将利用智能合约保证将资金优先用于支付应付账款,如服务费等。仅当收款人在完成合同规定义务时,平台才会

按照智能合约将其余资金转入收款人账户。平台通过智能合约既可保证参与交易的各方的切身利益,也杜绝了相关人员的干预,避免了数据造假和资金挪用等问题的发生。

广告活动被分解成 3 个阶段:

1)广告交易阶段(Ad Trading Phase,ATP)。该阶段包含广告主与广告服务商之间的在线招标、竞标、中标和订立合同的过程,广告主将直接与各个环节的服务商进行沟通,提升沟通效率。如果相同服务商以不同角色参与交易,则可捆绑签订制作和发布合同,优化交易流程。服务商可自主选择适合的广告主进行合作,查看广告主发布的广告需求和广告主评分历史,并在获得广告主授权后进一步地查看详细资料。交易过程的关键点将完整地记录到区块链中,其过程描述如下。

- 步骤 1 广告主发布广告需求。
- 步骤 2 服务商在需求池中查看广告需求并选择合适的广告需求投标。
- 步骤 3 广告主自愿选择是否为投标者开放更多资料的阅读权限。双方进入协商阶段(线上协商或线下协商)。
- 步骤 4 协商一致后广告主选择中标者。
- 步骤 5 由服务商填写广告服务合同(包括广告制作合同、广告发布合同)并签章。审核后将合同提交给广告主确认。
- 步骤 6 广告主签章确认合同内容。
- 步骤 7 服务商按合同规定时间和义务为广告主提供服务,广告主按合同规定预付货款。

2)广告服务阶段(Ad Serving Phase,ASP)。该阶段为广告服务商依据合同为广告主提供广告服务的过程,完全不干预其他环节。所有服务商在服务过程中产生的关键点信息都将写入区块链中。

广告制作者有义务按照合约内容上传制作成果,并将其其他相关内容交由平台审核,任何链接、图文、视频内容必须通过智能合约初审以及平台专员审核,在通过后转交给广告主确认。平台专员由所有节点分别派遣并为提交内容是否有效投票,只有超过 2/3 的专员确认通过的内容才被视为平台审核通过。广告制作者服务的过程如下。

- 步骤 1 广告制作者更新内容制作进度,直到作品完成。
- 步骤 2 广告制作者上传广告作品(文字、音频、视频等),在平台审核后将其提交给广告主确认。
- 步骤 3 广告主对广告作品进行确认,若不满意则可提出修改意见,返回步骤 1;若满意则确认接收。
- 步骤 4 经广告主确认后,平台按照智能合约为广告制作者支付尾款,交易结束。

媒体拥有者有义务配合平台提交参与服务的网站域名或其他渠道信息,以便平台自动核验服务效果,其服务过程如下。

- 步骤 1 广告主提交自备广告产品或使用广告制作者作品。
- 步骤 2 媒体拥有者调用平台提供的广告发布服务展示广告。
- 步骤 3 媒体提交网址或应用等信息证明开始履行广告

发布义务。平台服务返回检测结果,并由平台专员确认提交的网站或应用中包含平台广告发布服务,若不通过则需重新提交。

步骤 4 进入反馈阶段。个人传播者在这一阶段接受由广告主自行发布的推广任务,其过程如下。

- ①广告主自愿发布个人推广任务,设定推广目标、完成目标、份数等,并预付奖励金。奖励金将存入广告主账户用于任务完成后的奖励发放。
- ②个人传播者进入推广任务平台,选择推广任务。
- ③个人传播者按要求上传推广凭证(网址、图片、音频、视频等),由智能合约初审检查凭证是否满足任务规定要求(份数、材料种类等),通过后等待广告主审核。
- ④如果广告主审核不通过可填写驳回原因,进入步骤⑤。广告主审核通过后,智能合约自动发放奖励金,单次推广任务结束并写入区块链,双方相互评分。
- ⑤个人推广者按驳回原因修改提交的凭证,返回步骤④。如与广告主产生分歧,可联系管理员介入协调。

3)反馈阶段(Feedback Phase,FP)。

平台服务按照智能合约自主反馈信息给广告主,保证无人干预,防止反馈信息被篡改。广告主根据服务效果为服务商打分,平台会根据智能合约的履行状况与广告主的评分调整服务商的评级。评级是一个综合分数,包含多项指标,与广告服务商信誉、服务水平等硬性指标关联,影响其竞争力,评级过低的服务商将永久失去服务资质。同时,广告主的评分行为也将作为关键点存储到区块链中,防止广告主的恶意评价。

对于服务商的评级,平台使用智能合约进行自动化评价,每隔一段时间自动根据服务商的智能合约履行状况和用户评分进行计算,在兼顾效率的同时保证服务商评级的时效性。评级的时间间隔将由服务商的服务规模和已有评级共同确定,服务规模越大且评级越高的服务商因为其良好的信誉和服务水平,评级频率将更低,但最低不超过平台规定的最低限度,如一个季度。

反馈阶段的过程如下。

步骤 1 平台提供的广告服务持续自动收集用户浏览信息,并验证信息的真实性。信息按照反馈生成策略存入区块链中。

步骤 2 平台依托智能合约(定期、满足条件或一次性支付等)为服务商支付酬金,酬金将划入服务商账户。

步骤 3 广告主与服务商双方确认服务完成,货款由平台转入收款方账户,收款方可自由支取。

步骤 4 交易完成,服务双方相互打分。

上述 3 个阶段形成了一个完整的闭环,被称作一次广告过程刻画。一次广告过程刻画不仅能保证广告主在任意时间了解、掌握广告活动的进程,使广告数据透明可信,评分和评级机制还能对下一次的广告交易提供指导意见。一方面评分越高的服务商意味着更好的广告服务,另一方面,服务商也能够查询广告主的评分过程,以便确定广告主是否是合适的合作对象。

3.6 与场景结合的广告奖励机制

奖励机制既是促进和吸引广告交易各方加入平台并遵循模型规范流程进行广告交易的保障,也是提高广告传播效率、吸引广告受众点击广告和观看广告的有效手段。OAMVB 的奖励机制被设计为 3 个部分:内部奖励机制、个人推广奖励机制和受众奖励机制。

内部奖励机制的首要目的是通过让利和发放福利的方式促进广告交易各方主动了解模型规定的流程规范并配合实施,增加用户对平台的黏性,进而实现模型运行时的稳定性。在广告过程刻画中,模型检测每一个关键点生成的最低要求,对参与各方的效率和提供的内容质量不做限制。例如,广告制作者在更新制作进度时,因为没有更新动力造成更新缓慢、拖沓或者不更新等;交易结束后打分环节出现随意打分、恶意打分、不打分等问题。为解决以上问题,我们提出了按信息的丰富程度和及时程度为交易方提供奖励的奖励制度:在广告过程刻画中,以关键点为单位对该关键点进行健康度评估,记为 PH(Point Health),PH 值为 0~1 之间的小数,PH 值越趋近于 1 则认为节点的健康度越高。健康度的评估将综合关键点内指定的 N 项可量化指标,如评论的字数、更新速度、上传的图片分辨率、数量等,平台将根据量化等级为各项指标评级,并根据各项评分的所占权重 W_n 计算项目分 P_n ,最后综合计算出平均评分即 PH 值。各关键点所需的量化标准项目以及各项标准的量化等级由管理节点按照实际运营状况设置并通过共识后生效,各项评分的所占权重则根据平台最近两周内关键点健康度评估的平均值和各项评分的分布动态调整,以保证每一项评分的结果实时有效且完成难度相似,防止利益相关方利用评分规则,以舍弃部分项目质量为代价换取高权值项目评分的投机取巧行为。平台将在结算时根据参与方提交的关键点健康度高低为其发放奖励。针对广告主,其奖励(如赠送广告时长、广告次数等)由智能合约自动结算。针对服务商,其奖励为减少交易过程中产生的手续费缴纳比例。

个人推广奖励机制是针对个人推广者设立的。由于个人推广者不参与广告交易活动,仅参与个人推广任务,因此不适用于内部奖励机制,并且其主要收入是广告主提供的奖励金,推广任务一般较简单,但单次推广利润较低。为了鼓励个人推广者积极完成推广任务,平台设立了推广周榜、月榜、年榜

等榜单,并从个人推广任务服务费中抽取部分服务费设立榜单赏金奖励各榜单名列前茅的推广者,榜单运作由平台负责维护。除了上榜奖励外,所有个人推广者都将收到合作商家提供的代金券、打折券等奖励,完成的任务越多,奖励越丰厚。

受众奖励机制是 OAMVB 奖励机制的核心,其目的是结合普通广告受众的消费场景为用户提供急需的福利,促使用户主动观看广告的广告奖励机制。普通广告受众并非 OAMVB 的注册会员,但很有可能是媒体拥有者的会员或注册用户。我们通过与媒体拥有者合作,将媒体拥有者可提供的即时折扣与广告发布服务绑定,在用户付款或待付款时为用户提供自由选择。用户可以选择观看广告来获取当前欲购产品的折扣,或者抵扣某些内购服务的部分费用。例如:某游戏应用中开发者设置了人民币购买游戏内货币的服务,假设 100 游戏货币需要 10 元购买,用户在内购充值时可以选择通过观看广告的方式用 10 元的价格购买 120 个游戏货币,而一段广告的时长至多为 30 s。由于消费心理与行为现象都是以认知过程为先导的^[24],而消费者对广告的认识过程主要有展露、注意、记忆 3 个方面。我们在消费者进行购买操作前使用其欲购物品的折扣优惠吸引消费者的注意力,将其注意力从欲购物品转移到观看广告可以获得即得即用的福利这一过程中,从而提高消费者对投放广告的注意力水平。在相同的广告展现条件下,更高的注意力水平可以使消费者对广告内容拥有更好的认识过程,进而达到更好的广告效果。这一过程中,如果使用其他的分析方法精准地判断出玩家的兴趣爱好并作出精确推广,则推广效果将会比同类型的其他广告更为显著,这也可以成为掌握了大量用户反馈数据的广告服务平台未来可推出的核心付费服务之一。推而广之,平台与媒体拥有者的合作可以根据不同场景的需要做出相应的改动,使用户在通过观看广告换取即得即用的福利时获得更好的用户体验,从而提高广告推广的成功率。

4 模型评估

采用对照分析的方法对提出的在线广告投放模型进行分析。首先,通过与在线广告现存的一些问题做对比(见表 4),分析模型的优势能够产生与影响。更进一步,通过与现阶段提出的其他在线广告投放模型进行对比(见表 5),分析本文模型的优缺点。

表 4 当前面临的问题与模型给出的解决方案

Table 4 Existing problems and solutions oriented from model		
问题类型	细节描述	解决方案
数据安全	交易数据不透明	采用关键点完整记录交易整个过程,广告主可随时查看
	数据被篡改或丢失	使用平台提供的微服务发布广告,由平台直接获取反馈信息,无人干预
	不可抵赖性	采用广告联盟区块链,借助区块链记录了完整的交易过程,篡改成本极大,实现不可抵赖
	交易隐私	使用许可网络和 RSA 非对称加密算法,保证信息只对有必要的人可见
	交易安全	由智能合约自动执行,使用 CFCA 生成具有法律效力的电子合同,保证交易安全
用户参与度	沟通效率	取消多级代理,广告主直接与各级服务商沟通,提高沟通准确性
	广告主无法影响服务商的服务态度	通过评分评级与准入资格等与指标挂钩的方式促使服务商提供优质服务,听取广告主意见
	个人用户难以涉足广告领域	个人用户在提供必要的凭证后也可顺利入住平台,轻松加入广告交易活动
	个人推广	普通用户可参与到广告推广中赚取佣金,增加广告传播的广度
稳定性	服务可用性	节点由多个组织共同管理,符合要求的其他组织也可加入,稳定性较强
广告效果	广告受众对广告接受效果差	使用受众奖励机制引导受众自愿观看广告,通过即得即用的福利提升受众关注度
规则	不同数据标准导致数据孤岛	使用统一门户、统一服务接口,可实时共享、授权访问信息

表 5 本文模型与其他解决方案的对比

Table 5 Comparison of proposed model and other solutions

指标	adChain ^[11]	AdEx ^[12]	Google AdWords ^[7]	OAMVB
基于区块链 Blockchain-based	true	true	False	True
共识机制 Consensus Mechanism	AdChain Registry (based on POS)	POS	None	Improved PBFT
区块链类型 Blockchain Type	Public blockchain	Public blockchain	None	Consortium blockchain
参与者 Participants	Advertisers, Publishers, adToken Holders	Advertisers, Publishers, Users	Advertisers	Advertisers, Producers, Media Owners (Publishers), Individual Transmitters
多方合作管理 Multi-partner Cooperation Management	true	true	false	true
快速回溯 High-speed Trace to the Source	false	false	false	true
完整的广告过程 Complete Advertising Procedure	false	true	false	true
多级代理 Multi-level Proxy	true	true	false	false
评分机制 Scoring Mechanism	true	true	false	true
奖励机制 Incentive Mechanism	true	true	false	true
微服务 Micro Service	false	false	true	true
机器学习 Machine Learning	false	false	true	false
人工智能 Artificial Intelligence	false	false	true	false

表 4 从 12 个方面将本文模型与其他 3 个现有解决方案进行了对比,可以看出本文模型具有一定的独创性,博采众长。但本文模型与其他解决方案相比仍存在许多不足:没有使用机器学习、人工智能等技术辅助广告的投放,未实现精确投放,未调动参与各方的积极性,与公有区块链相比处于劣势等。

结束语 随着区块链技术的逐渐成熟,社会中越来越多的领域会逐渐将区块链技术应用到解决自身现有问题的研究中。基于在线广告的区块链已经受到了许多业界巨头的关注,成为最有望首先开始广泛应用区块链技术的领域之一。本文提出的基于区块链的在线广告投放模型能够帮助广告交易各方参与者快速高效地找到合适的合作伙伴,并且尝试对当前在线广告解决方案中出现的数据不透明、多层代理导致的效率低下、数据被篡改等问题提出解决方案,以满足越来越庞大的在线广告投放需求。

然而,基于区块链的在线广告投放模型在具体实现时仍然面临着许多挑战:

- 1)由于区块链技术仍在不断发展,很多已经成熟的技术与区块链技术融合时仍然存在障碍,如在区块链中高效地使用机器学习等技术等。
- 2)文中涉及的智能合约,如企业贡献度计算、企业节点间的分账合约等,仍然需要与实际情况结合做出更为详尽的设计。
- 3)文中涉及的关于分布式存储技术、许可网络、权限控制等设计细节仍待进一步完善。
- 4)文中涉及到的商业模式、运行规范等仍不尽完美,需要在后续研究和具体实践中进一步完善。
- 5)文中涉及的广告投放方式较为单一,有待进一步扩充。

参 考 文 献

[1] Dentsu Aegis Network. Advertising expenditure Forecast Report 2017-06 [EB/OL]. [2017-06-28]. <http://www.199it.com/archives/606519.html>. (in Chinese)

电通安吉斯集团. 广告支出预测报告 2017 年 6 月 [EB/OL]. [2017-06-28]. <http://www.199it.com/archives/606519.html>.

[2] YUAN Y, WANG F Y. Blockchain: The State of the Art and Future Trends[J]. Acta Automatica Sinica, 2016, 42(4): 481-494. (in Chinese)

袁勇,王飞跃. 区块链技术发展现状与展望[J]. 自动化学报, 2016, 42(4): 481-494.

[3] CASTRO M, LISKOV B. Pratical Byzantine Fault Tolerance and Proactive Recovery[J]. ACM Transactions on Computer Systems, 2002, 20(4): 398-461.

[4] SAM N. Building Microservices [M]. Sebastopol: O'Reilly Media, Inc, 2015.

[5] DONG L Y. The marketing model of Internet advertising in the era of big data[J]. Media, 2017, 19(8): 68-70. (in Chinese)

董丽荣. 大数据时代互联网广告的营销模式[J]. 传媒, 2017, 19(8): 68-70.

[6] LIU Y G, LI H F. Research on the marketing model of precision advertisement in the new media communication[J]. Contemporary Communications(Chinese Version), 2013, 34(4): 86-88. (in Chinese)

刘英贵,李海峰. 新媒体传播中精准广告的营销方式研究[J]. 当代传播(中文版), 2013, 34(4): 86-88.

[7] Google. Display Ads, Video Ads, Search Ads &. App Ads-Google AdWords-Google [EB/OL]. [2017-01-06]. https://adwords.google.com/home/#?modal_active=none.

[8] XU Z L, MA R. Programmatic Buying and the Change of Network Advertising Ecosystem[J]. Journal of Shanxi University (Philosophy &. Social Science), 2016, 39(2): 72-78. (in Chinese)

许正林,马蕊. 程序化购买与网络广告生态圈变革[J]. 山西大学学报(哲学社会科学版), 2016, 39(2): 72-78.

[9] GALLAGHER K. Ad fraud estimates doubled[EB/OL]. [2017-03-16]. <http://www.businessinsider.com/ad-fraud-estimates-doubled-2017-3>.

[10] ZHENG T J, TANG M Y, SONG D, et al. A assumption about application of block chain technology in advertising industry

[J]. Journal News Research, 2017, 8(13): 261-269. (in Chinese)

郑天娇, 汤明妍, 宋丹, 等. 区块链技术在广告业中的应用设想 [J]. 新闻研究导刊, 2017, 8(13): 261-269.

[11] MetaXchain, Inc. The AdChain Registry [EB/OL]. [2017-05-31]. <https://adtoken.com/white-paper.pdf>.

[12] GEORGIEV I, STOYANOV D, IVANOVA V. AdEx: A Decentralized Ad Exchange [EB/OL]. [2017-07-30]. <http://adex.network/adex/AdEx-Whitepaper-v.7.pdf?v=1.0.15>.

[13] HE P, YU G, ZHANG Y F, et al. Survey on Blockchain Technology and Its Application Prospect [J]. Computer Science, 2017, 44(4): 1-7, 15. (in Chinese)

何蒲, 于戈, 张岩峰, 等. 区块链技术与应用前瞻综述 [J]. 计算机科学, 2017, 44(4): 1-7, 15.

[14] WANG X G. Summary of the Consensus Algorithm of Block Chain Technology [J]. China Computer & Communication, 2017, 12(9): 72-74. (in Chinese)

王晓光. 区块链技术共识算法综述 [J]. 信息与电脑, 2017, 12(9): 72-74.

[15] NAKAMOTO S. Bitcoin: A peer-to-peer electronic cash system [EB/OL]. <https://bitcoin.org/bitcoin.pdf>.

[16] KÖLVART M, POOLA M, RULL A. The Future of Law and e Technologies [M]. Switzerland: Springer International Publishing, 2016: 133-147.

[17] DELMOLINO K, ARNETT M, KOSBA A, et al. Step by step towards creating a safe smart contract: lessons and insights from a cryptocurrency lab [C]// International Conference on Financial Cryptography and Data Security. Springer, Berlin, Heidelberg, 2016: 79-94.

[18] Wikipedia. Merkle tree [EB/OL]. [2018-01-06]. https://en.wikipedia.org/wiki/Merkle_tree.

[19] PRENEEL B. Cryptographic hash functions [J]. European Transactions on Telecommunications, 1994, 5(4): 431-448.

[20] COCCO S, SINGH G. 6 technical advantages of Hyperledger Fabric for block chain network [EB/OL]. [2017-12-06]. <https://www.ibm.com/developerworks/cn/cloud/library/cl-top-technical-advantages-of-hyperledger-fabric-for-blockchain-networks/index.html>.

[21] FAN J, YI L T, SHU J W. Research on the technologies of Byzantine system [J]. Journal of Software, 2013, 24(6): 1346-1360 (in Chinese)

范捷, 易乐天, 舒继武. 拜占庭系统技术研究综述 [J]. 软件学报, 2013, 24(6): 1346-1360.

[22] CASTRO M. Practical byzantine fault tolerance [M]. Massachusetts Institute of Technology, 2000.

[23] China Financial Certification Center. CFCA's digital certificate service agreement [EB/OL]. [2015-08-04]. <http://www.cfca.com.cn/20150818/101234477.html>. (in Chinese)

中国金融认证中心. CFCA 的数字证书服务协议 [EB/OL]. [2015-08-04]. <http://www.cfca.com.cn/20150818/101234477.html>.

[24] CHEN X R. Research on the source of actice effect in intensive advertising based on consumer cognition process [J]. China Economist, 2008, 33(11): 72-73. (in Chinese)

陈小荣. 基于消费者认识过程的密集广告积极效果来源研究 [J]. 经济师, 2008, 33(11): 72-73.