基本注意力代币(BAT)

基于区块链的数字广告平台

Brave Software

2017 年 5 月 8 日

摘要

数字广告已经崩坏了。曾经由广告客户，广告发行商和用户一度主导的在线广告市场已经被推翻了，造成这一结果的起因来自“中间商”广告交易所，受众分割，复杂行为和跨设备用户跟踪以及通过数据管理平台进行的不透明跨行业共享。用户面临前所未有的恶意广告和隐私侵犯的风险级别。移动广告给平均用户数据计划收费带来了每月高达23美元的费用，网页下载速度过慢相当于电池寿命直接减少了21%。作为应对，超过6亿个移动设备和台式机（全球范围）使用了广告屏蔽软件，而且这个数字还在增长。传统发行商在过去十年中已经丢失了大约66%的收入。发行商的收入下降，用户越来越感觉到被侵犯，广告客户评估效率的能力也下降了。我们的解决方案是基于区块链技术的去中心化，透明的数字广告交易所。其第一个组件是Brave，一个快速，开源，以隐私为导向的浏览器，它能够屏蔽第三方的广告和跟踪器，并构建一个能够根据衡量用户关注度来奖励广告发行商的帐本系统。Brave现在将介绍BAT基本关注力货币），这是去中心化广告交易所使用的令牌货币。它在保护隐私的同时根据用户的关注力来补偿浏览器用户。BAT连接广告客户，广告发行商和用户，并在被相关用户关注力主导的同时，消除与现有广告网络相关联的社会和经济成本，例如欺诈，隐私侵犯和恶意广告。BAT是一种支付系统，它奖励和保护用户，且可以为广告客户提供更好的转化，给发行商带来更高的收益。我们将BAT和相关技术视为未来Web标准的一部分，它能够解决发行商内容营利的重要问题，同时也保护了用户隐私。

Contents

1 价值定位

我们提议把BAT定义为一个存在于安全，匿名，自由加入的广告系统中的交易所使用的货币，这个广告系统是基于浏览器和移动应用程序网络视图的。BAT系统提供了：

- 用户：查看广告时的强大隐私性和安全性，改进的相关性和性能以及一部分的货币份额。
- 发行商：提高利润，高质量用户报告，和减少广告欺诈。
- 广告商：廉价用户关注度，减少广告欺诈，更好的数据归因。

2 绪论

> “注力被普遍认为是一种商品，就像小麦，猪胸肉，又或者是原油。现存的企业们很长一段时间都是取决于它来带动销量。而且20世纪的新兴产业也把关注力变成他们铸造的一种货币形式。从无线收音机开始，每一种新的媒体形式都会通过重新销售它们使用“免费”内容交换捕获来的关注力来达到它们自己的商业可行性。”-Tim Wu, Attention Brokers

广告技术（“ad-tech”）的前景是创造一个相对关注力来说更加高效的市场。希望互联网，这个最新的“新媒体”的降临，将伴随着透明和高效的广告市场。

理论上，卓越将得到回报。最好的新闻和娱乐将获得其相值得的关注力和投资。广告技术将“通过数据分析，即时估价和分配，使营销人员更接近用户。”数据将用于“准确地识别关注用户，确定关注用户的价值，并立即向他们传达正确的信息。”简而言之，用户的关注力将得到正确的重视。

但上述理论并没有发生。相反，过去二十年来发展过来的广告技术生态系统是一个充满令人困惑的各种中间人和复杂性的生态系统。更糟糕的是，广告技术为发行商，广告客户和用户带来了许多相关问题。用户已经失去了隐私，面临恶意软件的危害，为广告下载支付高额费用，网络下载速度慢。发行商损失了数十亿美元的利润，而欺诈行为却猛增。广告客户的报告和定位不准确。本文将回顾目前的广告技术现状和内容制作者的困境。它将概述一个新的解决方案，这个方案为发行商，广告客户和用户创建一个基于区块链的透明且高效的市场，准确地评估和奖励互联网内容的关键驱动力：持久的用户关注力。

2.1 低效而且问题百出的市场

Thomas Davenport和JC Beck指出，“关注力将心理活动集中在特定信息项上。信息项进入到我们的意识，我们考虑到一个特定的项目，然后我们决定是否采取行动。”[1]在这个意义上，关注是缺乏的一种形式，引起了一些我们将立即解决的基本经济问题。

广告在其整个的发展史上都被用作捕获关注力的主要机制，将关注上升到兴趣水平以煽动一些欲望，然后将其转化为行动- 也就是AIDA。[2] 最早的广告形式可以追溯到古代中国，埃及和中世纪的欧洲。随着19世纪印刷产品的增长，印刷形式的广告开始广泛扩大。仅仅包含广告客户，发行商和用户的这个市场仍然保持相对简单- 尽管有一些补充- 即使在新的媒体形式广播和电视出现后也是如此。

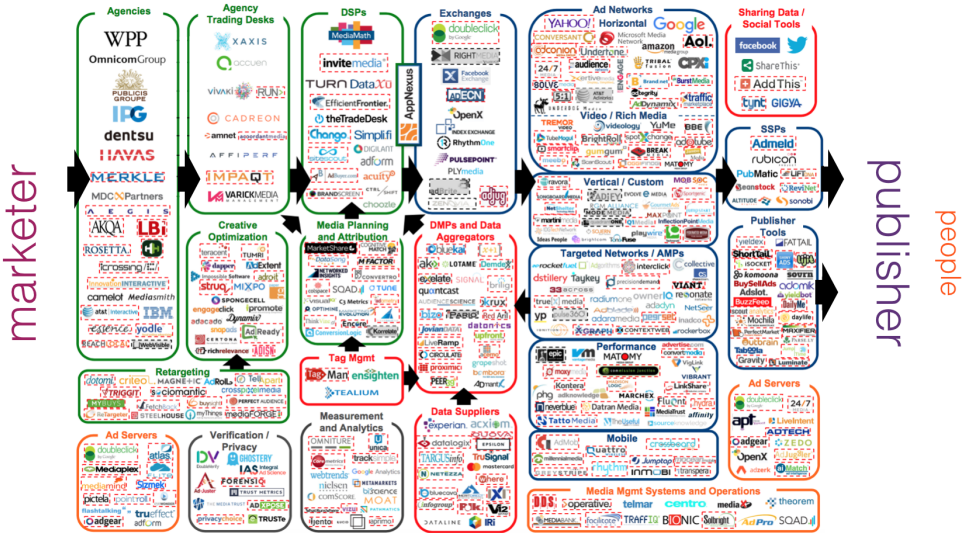
互联网的崛起带来了新一轮广告技术的发展，这个时候的广告市场前景是具有更快的速度和更好的信息，这两个关键因素有潜力从根本上提高关注力市场的效率。不知道怎么与直觉相反，有组织发展而来的复杂性和不透明度带来了相反的结果。系统不能正常工作。最大广告客户宝洁（P&G）的首席品牌公关人员最近表示：

> “给数字世界放行的时代已经过去了。是时候进步了。是时候行动了。”[3]

特别是在过去十年，随着更多的玩家直接或间接地从广告这块大市场分一杯羹，广告生态系统变得越加复杂和拥挤。生态系统的复杂性增加了广告客户方面数字营销团队人员和任务困难度，导致广告成本增加。在系统的另一端，传统广告发行商同时面临着无广告屏蔽器的关注力市场的萎缩，以及由在交易中扮演经济中间商角色的众多第三方玩家带来的广告收入缩小。

2.2 关注力市场

目前正在为品牌广告进行预算的销售计划者需要考虑到在广告和最终用户之间存在的大量中介人数。代理商，交易柜台，需求端平台，台式机和移动网络交换机，产出优化，富媒体供应商和合作服务通常会消耗制作广告和投放广告预算的大部分。负责包装品牌宣传活动的机构也常常使用数据聚合器，数据管理平台，数据提供商，分析学，测量和验证服务来实施欺诈，增强目标和确定归属。这些因素加剧了品牌广告宣传活动提供高效关注力所需要的高昂交易成本。



data source: www.lumapartners.com

发行商还面临广告服务接收方的大量费用和中间商。发行商支付广告服务费用，宣传组建的操作费用，部署和监控的运营费用，发行商分析工具的费用;他们也放弃了大量收入给了品牌广告客户通过电脑编程广告使用的同样一批中介机构。当恶意广告从交易所向忠实读者传播的时候，发行商面临用户投诉的直接损失，而他们通常很少甚至完全不知道恶意广告的来源，也没有从应该负责的交易所那得到帮助，即使应该是他们对允许这样的恶意广告在他们的广告系统中存在来负责。随着整个广告系统的整体复杂性增加了广告数量和广告花费，这些恶意广告减少了整个网络的收入。

这种复杂性还有隐藏的成本。单个广告单元可能会跨越多个网络，购买和销售端的广告服务器，验证合作伙伴和数据管理平台。发行商从每个中间商的交易中损失一部分收入。这些交易中的任何一个都会减损用户体验。许多中间玩家涉及数据传输，这也增加了延迟。通过页面上的脚本进行的任何传输都可以消耗用户的数据计划和手机的电池寿命。当这些后果最终发生时，用户经常会觉得他们的体验进一步损害了，其中混淆了许多分散注意力的令人困惑的广告队列，发行商允许放置这些广告是希望获得更多的收入。

此外，违反用户隐私确实会需要一笔显着的社会消耗;经济学家将违反用户隐私的行为比做相类似于环境污染。[4]据Pew Research称，“总共有91%的成年人同意或强烈认同用户对于个人信息如何被企业收集和使用完全失去了控制权。”[5]大多数人（64%）认为“政府应该做采取更多的措施来管理广告商“，关于他们如何使用和存储用户个人信息。这并不是什么奇怪的事，考虑到访问一个流行的媒体网站往往可以有着70个追踪器散漫的被设置在读者上。

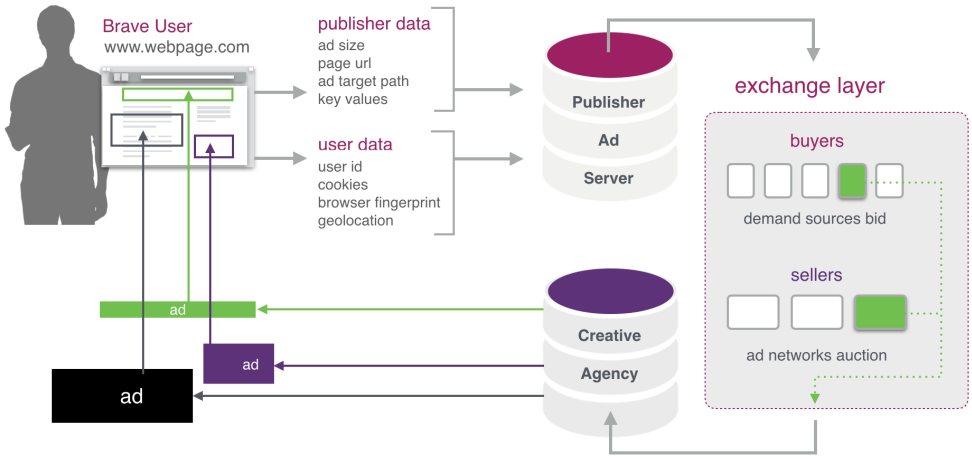


Figure 1: 传统数字广告流动

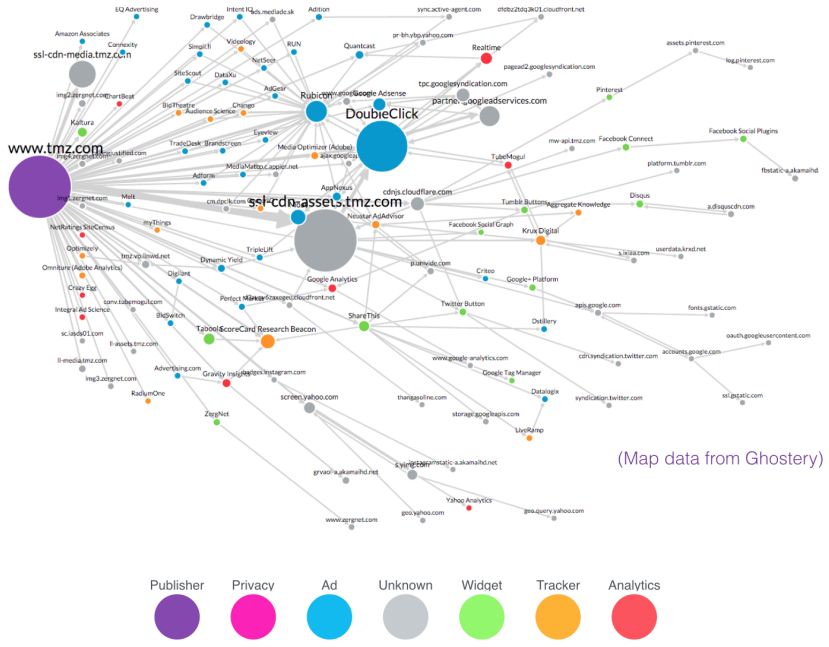


Figure 2: 内容网站上的传统追踪

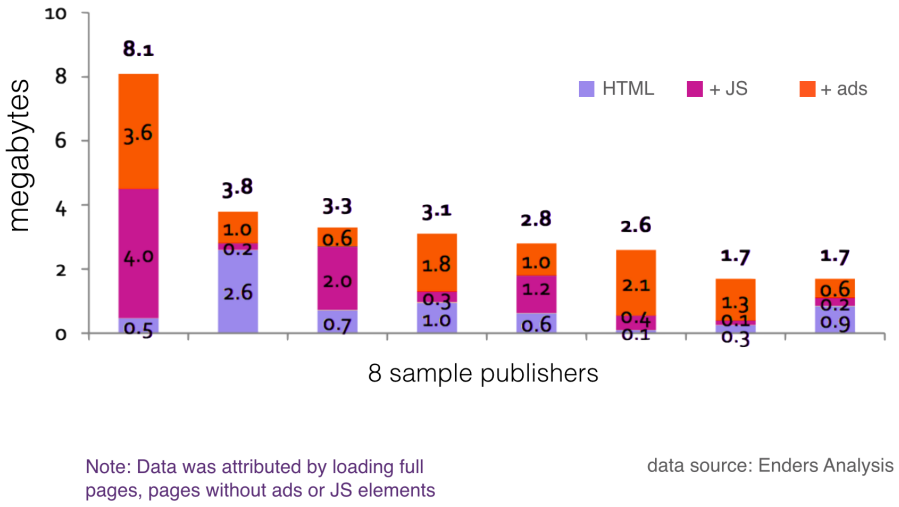


Figure 3: 新闻网站上通过数据元素传输的数据

欺诈也是附属在广告市场上的一个主要问题。黑客创建恶意机器人来产生欺骗广告客户的虚假网站。互联网上“机器人”远程控制的软件运行在受损的个人计算机或云计算基础设施上，他们被编程控制进行犯罪活动- 每年从广告业抽取数十亿美元。根据Business Intelligence：“这些机器人创建的网站充满了侵权的内容，并通过一个由受感染计算机组成的复杂网络生成假的交易数据。根据Association of National Advertises（ANA）和White Ops的报告，2016年互联网机器人创造的广告欺诈预计将消耗广告客户成本高达72亿美元，高于2015年的63亿美元。”[6]没有迹象表明这个级别的欺诈程度将会保持不变或者降低。

广告商面临着欺诈，而与此同时用户也遇到越来越多地恶意广告。恶意广告是一种假广告通过欺骗用户点击他们，然后下载恶意代码（包括勒索软件）。他们也可以引诱用户访问用于窃取财务信息的假域名网址。根据去年发布的RiskIQ报告，“从2015年到2016年，恶意广告的广告比率上升了132%。”根据Bromium[7],最常受到恶意广告攻击的网站是新闻网站和娱乐网站。

Web用户也不完全了解他们为查看广告的特权所付出的代价。根据Business Intelligence，一项研究表明访问主流发行商时，高达79%的移动数据传输是下载广告的结果。研究人员比较了在没有广告屏蔽器，有广告屏蔽器，和广告屏蔽器和JavaScript同时禁用的情况下完整加载页面时的数据使用情况。

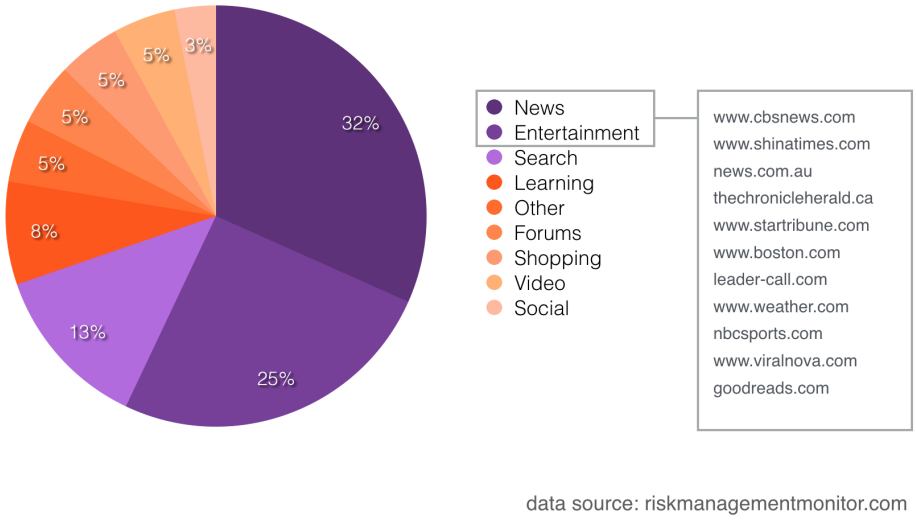


Figure 4: 被恶意广告攻击最频繁的网站

该文章指出研究人员得出一个结论，在测试期间，“移动数据网络上广告占发行商页面所使用的全部数据的一半”。一般的智能手机用户评价每月消耗1.8GB的流量。根据2Gb的运营商计划，这意味着平均用户最终每月需要支付23美元来下载广告，跟踪器，脚本和其他相关数据。[8]

“纽约时报”的一项研究发现，在50个顶级发行网站上广告使用的数据造成了相当大的下载时间和成本。其中最极端的例子是，www.boston.com花了30.8秒的广告加载时间和8.2秒的社会评论加载时间。研究文章得出结论，删除广告“在一次典型的单元连接中节省了超过五秒的加载时间”。加载广告的数据同样带来了财务成本- 广告内容的价格通常超过编辑材料的价格。

恶意广告，加载时间，数据费用，电池寿命和隐私损失这些加起来就导致了用户采用广告屏蔽软件。这进一步降低了发行商的收入，也使市场定位剩下的广告观众变得更难。

广告屏蔽器对于发行商而言是一个日益严重的问题。研究确认了使用广告屏蔽软件的用户更喜欢简单的无广告导航或几乎无广告的内容。

根据Pagefair的说法，超过6亿个移动设备和桌面设备现在正使用广告屏蔽。预计2017年将有866万美国人使用广告屏蔽器[9]。年轻的用户也相比更可能采用广告屏蔽技术，使得这种屏蔽技术的长期财务影响比其一开始看起来的问题更加严重[10]。

发行商的这个“完美风暴”在过去几年中变得越来越糟糕，因为Google和Facebook已经占据了越来越多的广告收入。他们声称加在一起拥有*73%*的在线广告收入和从*2015*年

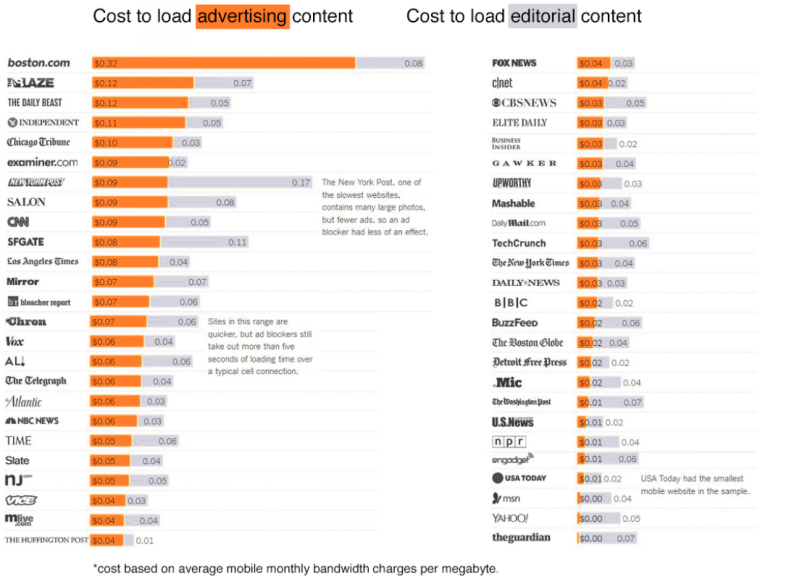


Figure 5: 内容加载消耗对比

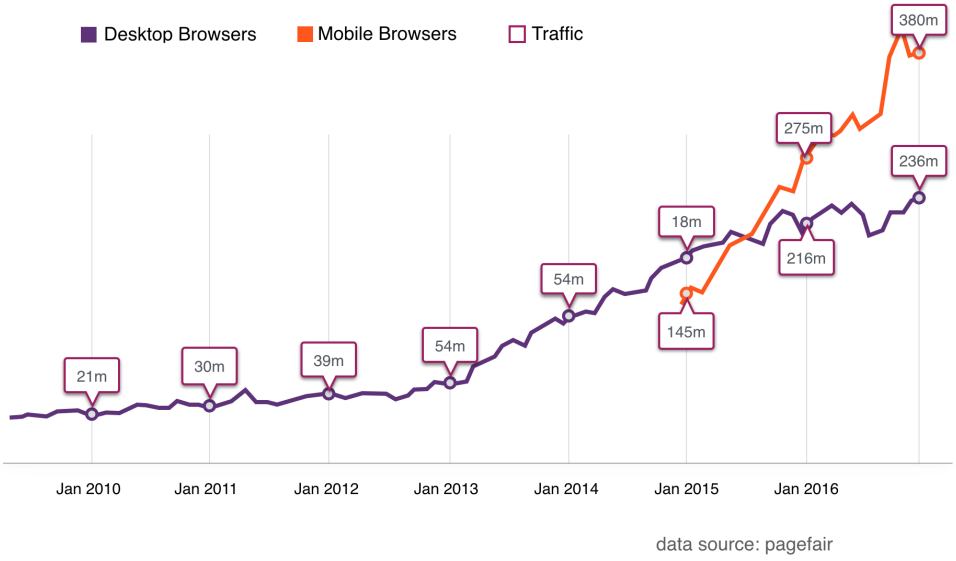


Figure 6: 使用广告屏蔽器的设备增加

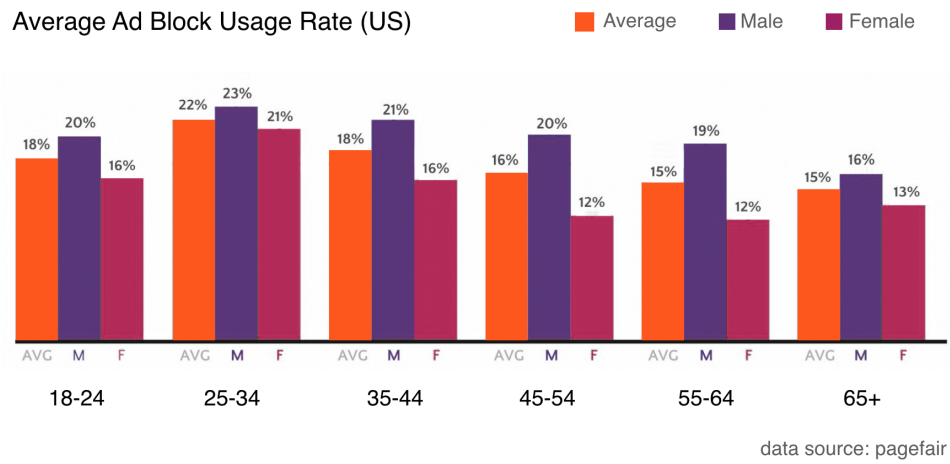


Figure 7: 使用广告屏蔽器的用户统计

到*2016*年美国整体广告预算中占有惊人的*99%*广告市场增长[11]。Google和Facebook给发行商带来的越来越多的关注力看起来似乎是一个净增值。但社交媒体驱动的传播质量相比直接链接来说质量更低。从社交媒体到达新闻网站的用户相比直接链接到达的用户通常只有三分之一[12]的时间进行到网页操作。分布式内容托管仅占有发行商收入的14%，其中大部分收入还是来自Youtube[13]; 许多发行商在这些平台上遇到严重的商品化问题。

这些平台上的广告客户也面临严峻挑战。平台庞大的规模使得它们变得不透明，变得很难评估其平台上广告活动的效率。由于大多数目标为这些平台的分析产品都是由平台所有者提供的，因此委托与代理的冲突出现了。有些广告客户认定来自围墙花园的传输相比其带来的问题来说是不值得的。有些人甚至仅基于一个第三方给出的分析，表示大部分的流量传输对广告商没有价值[14]。

为了扩大他们的围墙花园，并通过直接在发行商领域从用户那里获取的传输和数据来加强市场的主导地位，主要平台玩家已经开始提供替代的内容传送渠道，声称他们拥有激励机制和更快，更安全的用户体验。虽然Facebook Instant Articles，Google AMP项目和Apple News发布渠道最初被提供给发行商作为扩大覆盖面和可视性的机会，但它们最终减少了发行商对品牌叙述和读者关系的控制，并长期直接将关注力从发行商网站转移开来。

一般来说，广告发行业面临着一个现存的威胁。传统发行商几十年来收入一直在下降。创建针对点击进行优化的内容给发行商带来的压力导致了大篇幅文章的减少，调查新闻和外国政治新闻的缩减，并产生了令人遗憾的社会成本，被命名为“clickbait”。

U.S. Ad Revenues	Q3 2015	Q3 2016	Growth	Share of Growth
Google	$7.9B	$9.5B	$1.6B	54%
Facebook	$2.1B	$3.4B	$1.3B	45%
Everyone Else	$4.6B	$4.7B	$40M	1%
PWC/IAB	$14.7B	$17.6B	$2.9B	

data source: fortune.com

Figure 8: 广告收入对比Google VS Facebook VS 其他

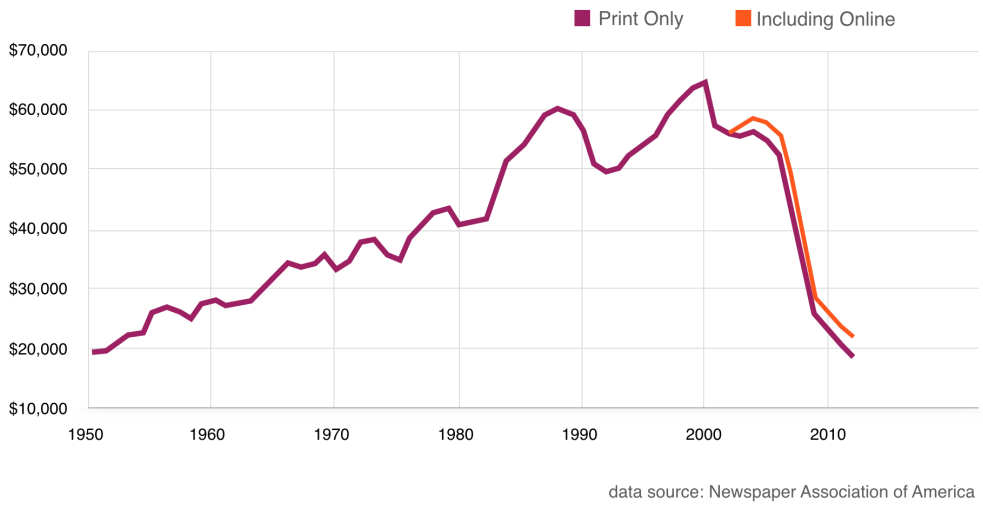


Figure 9: 报纸广告收入的下降

这种功能失调的动态已被整个行业所注意到。营销预算继续攀升[15]，但发行商的收入仍然是静态不变的或者是收缩减少的[16]。这体现了市场的严重低效，而这种低效可以用基于新技术的简化和高效经济体系进行修复。

3 新政：在区块链上基于注意力的经济学

中产阶级的多样性和对出版商和用户缺乏增值，使得当前在线广告生态系统的一些简单化变得不可避免。目前的趋势是向寡头垄断发展，诸如Google和Facebook等门户公司控制整个在线市场的预算，发布商没有能力控制其收入。此外，随着用户继续采用广告拦截技术，剩下的广告资助市场萎缩的结果似乎是不可避免的。

存在的现实是：用户的关注是有价值的，但它并没有被高效透明的市场体系合适的定价。虽然在互联网上产生的大量信息已经变的平淡无奇，但人类只能将有限的注意力集中某些小部分信息上。在现代社会，信息是相对便宜的。人们对信息的关注仅仅是少数。正如赫伯特·西蒙（Herbert Simon）在1971年一篇有影响力的文章中写道：

> *"...在信息丰富的世界中，信息的丰富意味着某些东西缺乏：信息消费的稀缺性。什么信息消费是相当明显的：它消耗了其接收者的注意力。因此，丰富的信息造成了注意力的匮乏，和需要在可能消费的过量的信息来源中有效地分配注意力。"*

最终，出版商提供可能对用户有价值的信息。用户以他们注意的重要信息作为对出版商的回报。目前，出版商通过广告网络和其他此类工具中介玩家的复杂网络将注意力货币化来实现营利。出版商不是通过用户的注意直接得到收入。出版商实际上是由用户注意的广告间接地得到支付的。在平面广告行业中，出版商习惯使用这种模式，但由于上述许多原因，网络广告仍然存在问题。用户受到当前广告生态系统的负面外部影响。

因此，用户遭受一种“电子污染”，包括安全威胁、隐私威胁、低效下载时间的成本、额外的移动数据费用的财务成本，以及许多广告的情况下，他们注意的成本过高。人的注意力是可以用尽的，直到多巴胺水平恢复。神经元可以并且会学会忽略广告位（所谓的“横幅失明”）。归根结底，滥用用户注意力和永久性损失用户，通过对广告位选择性失明和广告拦截器的采用，引起了与替代品（如猪肚或原油）不同的关注。虽然大多数用户可能愿意为访问发布商的信息支付一定的价格，但是当我们总结当前广告生态系统强加的负面外部性时，用户的注意力的定价是错误的。

3.1 基本注意力的度量（BAM）

为了提高数字广告的效率，需要一个新的平台和交换单位。第一阶段涉及推出一种新的浏览器，Brave，即一个快速，开源，注重隐私的浏览器，阻止广告侵入和跟踪的浏览器，它包含一个分类帐系统，可以匿名地衡量用户的注意力，以准确地奖励发布者。下一阶段涉及引入基本注意代币或BAT。这是一个为了能实现去中心化广告交易的代币。BAT连接广告商、发布商和用户，创建一个新的、高效的市场。该代币基于Ethereum技术，一种基于开源、基于块链的分布式计算的智能合约平台。这种加密算法保证了智能合约是存储在Ethereum块链中的有状态应用程序，具有完全强制执行的性能。代币来源于-或被命名为-用户注意力。在这种情况下，注意力只是集中在精神参与-在一个广告上。

在浏览器中私密监控用户意图的能力允许丰富的度量用户关注指标的开发。例如，展示是否已投放到活动标签并衡量活跃用户参与的秒数是知道的。在浏览器的活动标签中查看内容和广告的实际时间才被衡量。在广告的任何直接投入之前，广告的注意价值将根据相关内容的增加持续时间和像素来计算。随着系统的完善，我们将进一步定义匿名的每个动作的成本的模型。

无论用户数据从外部模型中提取和监控多少，设备间学习都会将真正相关的广告与内容进行匹配，用cookies从中间人和第三方跟踪都无法实现。这些外部模型仍然无法简单地跟踪交易，不足以为用户经常购买的产品投放广告。通过真实的反馈机制进行交易的用户参与可确保选择采用BAT获得最有可能转换为交易的最佳的匹配产品。最终归结为对用户的信任和尊重。通过仅将数据保存在设备上，加密数据并屏蔽用户身份作为核心原则，BAT与用户建立联系，证明不仅数据储藏价值，而且具有在当前的行业模式中被中间人逐年被利用和被忽视的实质价值。

Brave捐赠者系统已经尝试了几项评分算法，它自动捐赠与网站的注意力成正比的数额。

建议的其中一个指标是活动窗口中的广告内容总共5次，每次至少5秒。这个特点的点击在移动窗口中计算30天。

另一个建议指标是“凹”评分[17]。这是一个因为一个阈值和开放和活动页面花费的时间量的有界功能而奖励一个出版商的的分数。例如，对于页面的两秒视图，可以授予一个“点”，对于30秒视图具有两个点，对于60秒视图具有3个点，对于较长视图而言具有递减或有限的回报。

目前实施的凹点评分，正用于向出版商分配以注意力计量为门槛的捐赠，这是一个时间有限的二次方分数。公式如下：

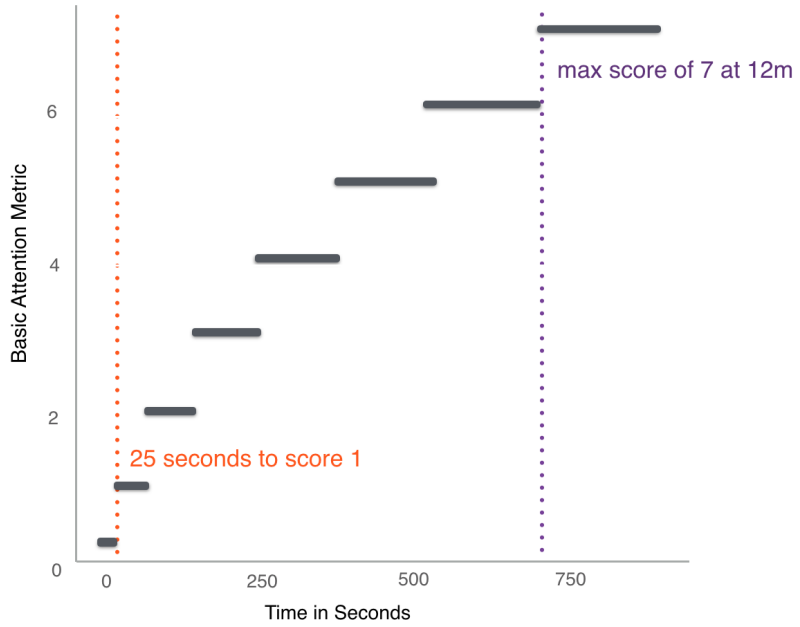


Figure 10: 基本的注意力指标度量

$$score = \frac{-b + \sqrt{b^2 + 4a * duration}}{2a}$$

其中$a = 13000, b = 11000, \Delta$ 以毫秒为单位。这给出25秒的最小门槛，以取得1分。给一篇文章设置上限为大约12分钟的注意力，给定的内容的最大分数是7分。

目前实施的BAM的节点：

另一个潜在的指标是基于在广告合作伙伴端购买的关键字的一部分的有针对性的广告，结合注意力指标，基本上将注意力与广告话题一起销售。

我们期望发布商和广告客户提出新的用户关注度量表，并且再我们向前推进项目时鼓励其他供应商建立主题。

3.2 代币技术

基本注意力代币（BAT）是基于以太坊（Ethereum）的代币，是新市场的重要组成部分。Ethereum是面向智能合约的开源的、基于块链的分布式计算平台。Ethereum是一种有效的分布式虚拟机，允许最终用户为交易构建智能合约。智能合约是存储在以太坊区块链中的状态应用程序。这些合约有加密算法保障安全的，可以验证或强制执

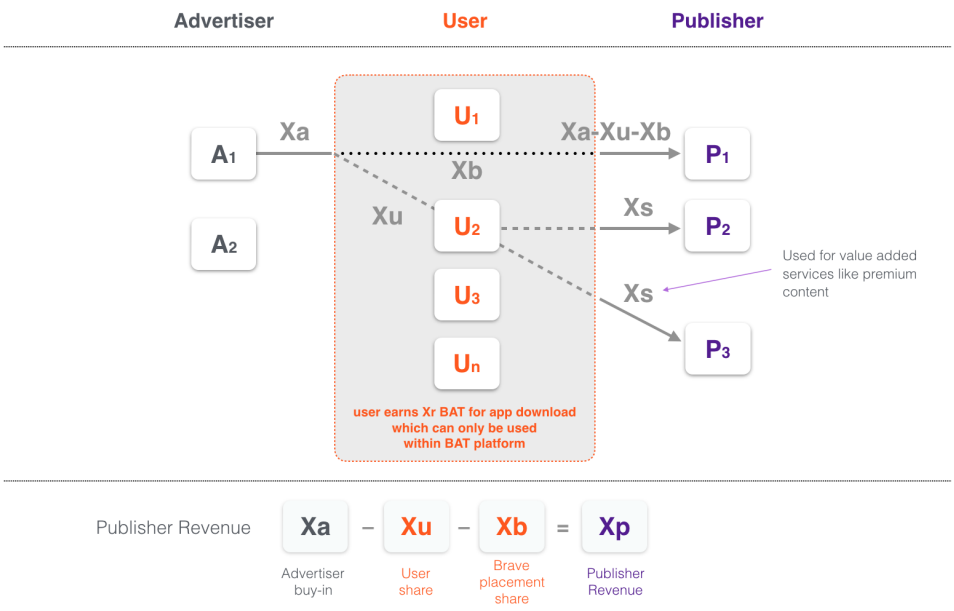


Figure 11: 基本注意力代币的价值流

行合约。代币合约是以太坊生态系统的标准特征。

以太坊已被用于移动支付系统，分布式交易所，与商品和法定货币挂钩的代币，市场清算机制，分布式计算资源的微支付系统，商品和证券交易所，众筹，和法律文件验证。大型公司已经投资并部署了以太坊，摩根大通，德勤，IBM，桑坦德银行，微软，卢森堡证券交易所以及苏格兰皇家银行都是关键的早期采用者。

使用BAT的微支付将使用Brave微支付分类账户完成第一阶段部署。每个在浏览器使用BAM浏览过的广告将进行验证。

此流程显示了BAT支付的概念流程。BAT支付系统的流程将不会在BAT支付系统的第一次迭代中精确地遵循该图表，因为支付将由Brave分类帐系统进行调整，但总体效果将相同。高层次的概念是广告客户向锁定状态Xa的用户发送代币中的付款以及投放广告。当用户查看广告时，支付的流量解除锁定，为他们自己的钱包（Xu）付保留部分余额，并将支付的份额传给brave（Xb），并将剩余部分转交给出版商（Xa-Xu -Xb）。

BAT将在早期阶段与经过验证的发布商一起特别绑定到Brave浏览器和Brave服务器。广告欺诈将通过发布源代码和加密算法保障交易安全来防止或减少。用于个人浏览器/用户的广告也将受到速率限制，并与活动窗口和标签相关联。在BAT中的支付将只发送给发布商，但是在一个发布商查看广告的付款可能会在另一个发行商使用，或

者通过BAT系统提供一些其他的优质服务。

3.3 用作发布商付款的代币

发布商付款将通过BAT系统支付。对于BAT的首次部署，BAT中的交易将通过Brave分类账系统进行，该系统是目前部署的开源零知识证明方案，以允许Brave用户使用比特币作为交换媒介向发布商发出匿名捐款。Brave的分类帐系统使用ANONIZE [18]算法来保护用户隐私。

对于BAT的第一个化身，BAT中的所有付款都必须具有发布商终端。发布者客户端 如今已经开发，已经如上所述测量了用户的注意力。“凹”奖励机制基于用于打开和查看页面至少25秒的固定阈值计算注意力分值，以及在页面上花费大量的时间的上限分值。然后将用户行为概要发送回Brave分类账系统进行记录并且基于分值进行支付。

在后端部署BAT所需的大部分基础设施目前正在编码完成，并且基于用户的注意力用于分发捐赠。因此，这种基础设施将根据测试用户和广告客户的反馈被尽快用于部署BAT。

一个完全分布式的分类帐是需要的，无论是为了公共责任还是潜在的可扩展性原因。BAT的出版商，广告客户和用户将鼓励使用这样的系统来跟踪BAT系统中的付款。

当使用正确的匹配算法时，状态通道允许具有强匿名保证的多样化的小交易。虽然Raiden和其他政府渠道计划与以太坊生态系统结合在一起，而如Zcash和Monero等新的区块链则通过快速增长的功能组合来提供更强的隐私保护，但解决这种交易的独特问题的新方案很可能将是用于BAT的大规模多方转账。

可以使用彩票系统，其中小额付款是概率性的，支付基本上以与硬币挖矿工作相同的方式进行，而工作证明[19, 20]，BOLT[21]，零知识SNARK[22]或STARK[23]算法不可能成为此栈的一部分，用于保护参与者的隐私。BAT情况得到缓解，因为浏览器客户的隐私至关重要; 发布商和广告客户的隐私权较少。在完全分布式的BAT系统中的交易几乎总是一对多，多对一，因此这种安排可能会提出新的零知识交易。

随着Brave演变成完全分布式的微支付系统，我们期望其他开发人员使用我们的免费的和开源的基础架构开发自己的BAT使用案例。我们希望BAT和与之相关的工具最终成为未来网站内容开发的重要Web标准。查看网页内容的发布商、广告客户和用户应享有私人的、安全的和设计良好的未来。

3.4 用户应用程序的代币

随着用在BAT中获得的一些广告支出，它们将成为广告和出版业经济中重要和积

极的一部分，而不是像现在这样被视为被动参与者。然而代币可以捐赠给个人内容提供者和发布者，但是代币的使用例子是任意数量的。

一个明显的使用例子是针对非常具体目标的广告。许多小企业人士都有适度的需求，他们需要通过他们正常的浏览活动获得的代币得到很好地服务。用户还可能会因为低门槛的高度针对性的广告而发现新用途; 例如针对宗教或亚文化人士的个人广告。

一些发布商可能会拥有通常只向订阅者提供的优质内容。由于订阅模式通常不会被互联网用户所青睐，这可能会为优质内容的提供商带来新的收入。也可以使用代币为朋友购买内容; 如果有人喜欢优质的文章，他们可以进行小额支付，将优质内容发送给他们的朋友们。

也可以向用户提供更高质量的内容以进行BAT交易。例如，娱乐频道上的较高质量的视频或音频，或新闻来源的某种新闻头条摘要。新闻或其他信息来源中的视频或音频内容可能仅限于进行小额付款的人员。

评论可能会使用BAT代币进行排名或投票，类似于某些评论部分的“点赞/鄙视”。由BAT认为支持的评论可能会获得更多的可信度，因为有人关心足够的支持的评论，会是有限的代币供应，以及代币传输可以被验证为来自真实的人而不是机器人。为了减少一些最低限度的付款也可以购买发布评论的权利，以减少滥用评论的数量。

最终，可以在Brave的生态系统中使用BAT来购买数字商品，如高分辨率照片，数据服务或仅需一次性的发布者的应用程序。许多发行商可以访问有趣的数据集和工具，而这些数据集和工具无法以订阅形式营利，但个人可能希望偶尔使用。例如，Pro Publica，Citzen Audit和Gartner等公司包含有趣的公共数据和优质内容，但是许多人发现订阅费用太高。那些不想购买访问权限或者订阅整个文档的用户可能对一小部分新闻感兴趣。

BAT可能还可用于Brave生态系统中出版商提供的游戏中。虽然这些应用程序目前不受出版商的欢迎，但许多平台提供商已经托管了有利可图的游戏应用程序。它可以和内容一起创造一个应用程序创建者的新经济。例如，“按压政治/娱乐人物图像”的游戏与评论文章一起。人们不会拿出信用卡来使用这样的应用程序，但他们可能愿意在正常的浏览活动中获得一些价值，以享受按压他们最喜欢的娱乐人物图像的快乐。

新闻提供者可以提供定制新闻预警，以便在生态系统内小额支付BAT。这些新闻预警对于关注当前事件、财务新闻或某些预期事件的个人来说可能是非常有价值的。

3.5 路线图

- 前1.0 BAT阶段：Brave已经有一个匿名的分类帐系统，用于根据用户的关注向发布商捐款和付款。使用ANONYZE算法确保客户隐私的安全保险库是BAT系统的

重要部分，已经在Brave中部署并运用。Brave已经在浏览器上测量用户的注意力，并向使用该系统的发布商分发捐款。

- 1.0 BAT：BAT钱包与Brave浏览器集成。由Brave的内部零知识证明分类帐系统处理的验证和交易，以保护广告客户，发布商和第三方的个人用户匿名性。广告资源将被重新定价，交易将根据报告的基本注意力指标（BAM）数据计算。

- 超越1.0 BAT：使用具有零知识证明协议的状态通道方案，在Ethereum上完全分布式的传输和验证过程，以确保用户隐私。根据广告客户反馈添加备用BAM指标。这将允许完全的用户隐私以及广告客户，用户和发布商的去中心化的审核跟踪，以确保他们收到通过BAT网络发送广告的正确金额。

- 浏览器作为平台/ BAT：根据需要，基于广告客户反馈更进一步的BAM指标。在BAT基础架构上构建应用程序的合作伙伴。此外，在这一点上，我们计划探索可通过BAT在浏览器平台上向用户提供的增值服务。

4 商业现状

4.1 竞争

- Reddit Gold 是Reddit 的高级会员计划，通过提供高级功能使付费用户获得更好的体验。Reddit 是主要的（广告）发布商，但这个项目是由Reddit 开发也局限在Reddit 平台。它不会提供能让广告发布商和用户通过区块链的代币来获利的机制。

- Steem 是社交媒体和博客平台，用户在收到点赞时可以赚取收益。这是一种货币化的Reddit 社区。Steem 确实使用区块链技术，但它不是广告发布商和用户获得内容奖励的通用平台。简而言之，它不是一个基于区块链的数字广告平台，它限定于Steem 平台。

- Blendle 是新闻业的iTunes，整理众多文章故事的内容，让读者挑选感兴趣的内容，可以为单篇故事小额付费。Brave 浏览器和BAT 不会策划任何内容。用户只需在网络上开展业务，广告发布商即可获得奖励。Blendle 不是一个基于代币的数字广告平台。

- 谷歌是一家搜索公司，其大部分收入来自广告。谷歌是现有数字广告生态系统的核心。他们受益于定义它的复杂性和不透明度。BAT 旨在授权那些收到的用户和

广告发布商的收益低于他们应得的收入。谷歌没有基于区块链的代币系统来提供奖励。用户通常不会意识到使用谷歌会侵犯他们的隐私。

4.2 BAT 优势对比表

生态系统现状	BAT 代币广告支付
加载慢	加载快
封闭限制	免费软件，开源的基础架构
浪费带宽	带宽开销低
界面杂乱	界面整洁
无关的广告	用户感兴趣的的广告
安全问题	没有恶意软件
可见性问题/权限	安全属性/关注度分数
广告客户交付不确定	交付确定
CPM /基于点击率	基于关注度
读者的关注度是没有价值的	读者的关注度会获得奖励
发布商收益低	发布商收益增加
中间人导致广告购买费用高	高效购买广告
复杂/昂贵可视性指标	简单/免费可视性指标
侵犯用户隐私	不涉及用户隐私

4.3 BAT 概述

The Basic Attention Token（BAT）旨在解决破碎的数字广告市场。BAT 是构建在以太坊之上ERC20 标准的代币，它将成为一个基于区块链的数字广告平台的全新的，去中心化的，开源和高效的交易单位。在生态系统中，广告客户将根据用户的关注度为发布商提供BAT 代币。参与的用户也会收到BAT 代币奖励，他们可以将其捐赠给广告发布平台，或者自己在平台上使用。这个透明系统将在提供少量且相关性更高的广告的同时，保护了用户数据的隐私。广告发布商能在提高其奖励比重的同时，降低被欺诈的概率。而广告客户也可以获得更好的报告和效果。该解决方案的第一部分——Brave浏览器已经可以运行。Brave是一个快速，开源，以隐私为导向的浏览器，可以阻止侵入式广告和跟踪器，并包含一个分类帐系统，可以匿名地衡量用户关注度，以准确地奖励发布商。下一步是引入BAT 代币机制。

目前，我们计划在Brave 浏览器上使用BAT，其他开发人员也可以自由使用其他浏览器。

Brave不仅仅是一个浏览器：它可以保护您设备上的数据，并在客户端加密之后在不同设备之间同步您的个人私有的浏览器配置。我们通过机器学习对你设备上的数据进行研究和抽象，为您提供隐私和匿名选项，为你的关注度提供补偿。Brave 浏览器去除了所有第三方追踪者和中间人，消除了数据泄露，恶意软件风险和过度收费。Brave 浏览器做到这一点，同时为发布商提供比现有低效率和不透明市场收到的收入大得多的收入份额。

因此，Brave 浏览器旨在重新设计基于在线广告的Web生态系统，为广告客户，发布商和客户提供一个双赢解决方案，其组件和协议可以成为未来的Web 标准。

4.4 主要团队成员

- Brendan Eich，首席执行官，Brave 浏览器联合创始人，JavaScript 之父，Mozilla 基金会和火狐浏览器联合创始人。
- Brian Bondy，主管开发人员，共同创立了Brave 浏览器。曾就职：可汗学院，Mozilla 基金会，印象笔记。
- Scott Locklin，高级工程师，共同创立了Kerf 软件。机器学习，预测与计量金融。
- Bradley Richter，设计主管，曾就职：EFI / Fiery，联合创始人：eBeam＆Luidia，Percipo。对Circullio 提供咨询。
- Catherine Corre，传播主管，曾就职：AOL（美国在线），Netscape（网景公司）。
- Marshall T. Rose，高级工程师，曾就职国际互联网工程任务组（IETF），参与SNMP 协议制定。
- Brian Johnson，高级工程师, 曾就职于JD Power 和Korrelate。
- Luke Mulks，高级广告技术专家，为技术事件回应，调查，支持和问题解决方案提供广告技术和Brave 浏览器。
- Aubrey Keus，高级工程师，曾就职：Pulse360（一家数据驱动广告技术公司）。
- Yan Zhu，EFF研究员高级工程师。曾就职：雅虎, Tor 项目, HTTPS Everywhere（强制https访问的浏览器插件）, Privacy Badger（屏蔽网站跟踪信息插件）。

5 附录

5.1 一个更有效的市场：科斯定理

经济学家研究了涉及社会和交易成本的问题。因为罗纳德·科斯在射频资源分配方面的工作[24]，他在1991年获得诺贝尔经济学奖。广告技术中的现代问题可以使用科斯的理论和之后对科斯理论的评论解决。目前，过度复杂的广告生态系统的影响是对用户的负外部性或“社会成本”。用户的隐私被侵入，浏览体验受破坏，甚至移动设备上的互联网带宽的有限供应也被目前生态系统的现状所消耗。用户关注的市场已经明显的变得无效率; 广告商购买注意力的交易成本太高。

广告屏蔽技术的广泛使用也为出版商带来了负面的外部性。如果每个人都阻止了广告，那么在发布商停止发布消息时，用户注意力可以交换的内容将很少。一个有效的注意力市场将消除这些负面的外部性，或以有效的方式对交易的所有各方进行补偿。

科斯定理指出，外部性交易或“社会成本”是存在的。如果交易成本足够低，信息对称性和产权明晰，议价可以达到帕累托效率的结果，而不管财产的初始配置如何。科斯定理的标准教科书示例由一个产生污染作为制造过程副作用的工厂，以及一个遭受污染的邻近土地所有者组成。

在邻居拥有污染权的情况下;

$$Q = 1 - (P + c)$$

c 是生产的边际成本，P 是允许污染的价格，Q 是在这个案例中的制造商的边际成本函数。邻居对清洁环境估价ν ，以及出售的Q污染许可证需要ν 的损失$Q = \nu(1 - (P + c))$所邻居以净收益最大化的原则发现污染排放许可的价格。

$$\max_P\{(1 - (P + c))P - \nu(1 - (P + c))\}$$

效益最大化是

$$1 - 2P - c + \nu = 0$$

给出的价格是

$$P = \frac{1 - c + \nu}{2}$$

和工厂购买的排污数量

$$Q = \frac{1 - c - \nu}{2}$$

如果工厂拥有完整的产权，邻居有效地从不使用的工厂购买一部分污染权。邻居想要购买$Q = 1 - (P - \nu)$ 单位。工厂最大化其净利润

$$\max_P\{(1 - (P - \nu))P - c(1 - (P - nu))\}$$

工厂的利润最大化是

$$1 - 2P + \nu - c = 0$$

所以价格依旧是

$$P = \frac{1 - c + \nu}{2}$$

科斯定理要保持均衡，它需要明确的财产权。根据定义，用户的注意力是重视数量。用户可以决定阻止特定发布商的广告，或选择放弃与发布商的互动。

这使得显而易见的是，事实上，注意力属于用户，但是不能阻止出版商和广告公司在法律上声明对用户注意力的所有权。即使在法律上需要用户关注的普通情况下，事实上，用户仍然拥有自己的注意力。例如，在航空公司飞行中给出安全演示时需要注意力，但是人们经常忽略它。

科斯定理的达到均衡的有效性的另一个要求是信息对称。发布商、广告客户和用户之间的信息不对称在现有的广告生态系统存在一段时间，但是从广告拦截器的使用越来越多看到，用户端的信息不对称正在瓦解。

目前，广告商和出版商在用于由不符合一方或双方利益的中间商管理者直接或间接评估宣传活动成效的大多数指标是严重的信息不对称。复杂的“可见度”指标会在广告客户和发布商之间产生不必要的冲突。这种信息不对称不是技术原因；它可以通过更好的技术，特别是在所有数据可以私下测量和匿名确认的端点的浏览器技术来解决。

最终要求是对于科斯模型的分析在产权明晰的情况下软性要求是低交易成本。科斯模型的交易成本是指涉及有争议的社会成本适合所有交易方的谈判交易的成本。在现有生态系统中，交易成本是很高的，广告客户、发布商和用户无法达成一致。

在我们当前广告网络的例子中，我们在发布商和用户之间有一个潜在的科斯模型交易谈判，对广告客户也有更好的结果。针对发行商和用户关注经济效率低下的科斯模型解决方案是广告客户通过用户对发布商的实际注意力来支付给发布商。

广告商因为用户向发布商支付的宝贵注意力的一部分将向发布商付款。读者也将因为他们宝贵的注意力直接得到回报。隐私侵害的“污染”，浏览速度慢和数据成本几乎可以完全缓解。广告商将知道他们的信息在没有诉诸关于“可见度”的复杂论证的情况下是否被传播。出版商将不用面对由广告拦截器采用日益增长而引起负外部性的问题。

浏览器还提供了更丰富的数据库，用于了解个人用户感兴趣的内容。Brave浏览器将包含用于评估用户兴趣的选择性和透明的机器学习算法。虽然针对金融发布商的广告活动可能对发布商的整体读者群体的广泛兴趣有价值，但可以为个人的或个人偏好的读者制定广告。

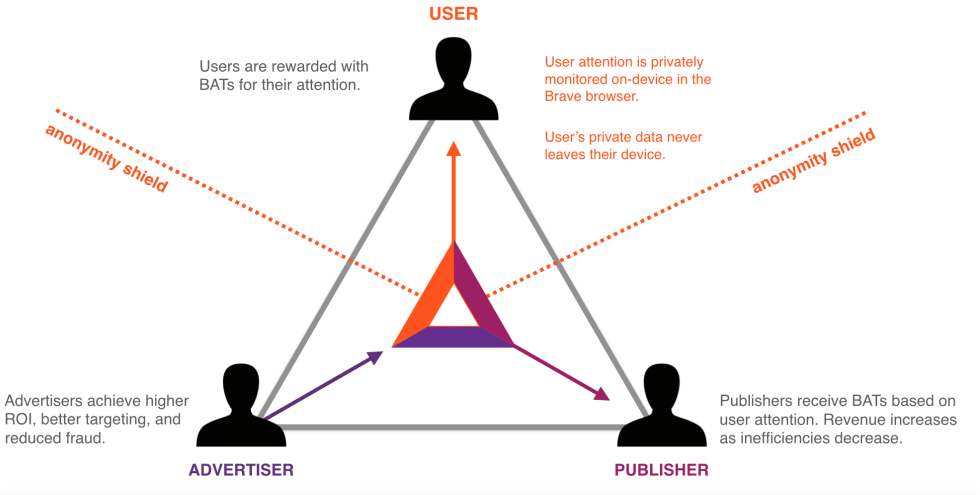


Figure 12: BAT数字广告流程

浏览器还提供了更丰富的数据库，用于了解个人用户感兴趣的内容。Brave浏览器将包含用于评估用户兴趣的选择性和透明的机器学习算法。虽然针对金融发布商的广告活动可能对发布商的整体读者群体的广泛兴趣有价值，但可以为个人的或个人偏好的读者制定广告。

例如，向贴近市政债券市场的人发送折扣债券经纪广告。正在阅读科技股和对市政债券不感兴趣的用户不会收到广告。广告客户将有效地瞄准他们有兴趣接触的精确点。当用户的兴趣不变时，用户将会收到更多相关的广告，且私人兴趣不会泄露给发布商或广告客户。

用户注意力应具有货币价值的想法对于发布商和广告客户都是熟悉的。出版商，特别是因为用户的关注而直接得到出版商回报的想法是新颖的。由于用户的注意力是有价值的商品，所以因为用户的关注而得到补偿是具有经济意义的。人们可以证明这是对广告生态系统对用户外部性的进行补偿。人们也可以通过这样一个事实来证明这一点：如果一个人得到补偿，一个人更有可能执行一个行动。用户的实际关注是通过在该广告位上添加基于块链的加密合约来发给发布者的也可以证明这点。代码是开源的，可由研究人员和对广告客户和发行商感兴趣的各方进行审核。

由于首次部署BAT的交易将通过Brave 分类账进行，Brave分类账通过设计具有隐私和确定性的用户匿名性，因此可以在保持用户隐私的同时实现全面的透明度。虽然这种集中式解决方案应该实现经济和技术目标，但为了进一步推进，可以开发去中心化的解决方案，以实现无需信任的可审计的交易。

对广告商来说，向查看发布商内容的用户付款看起来可能是异端的，但现实是广告客户正在向某人付款。删除对用户/发布者关系没有价值的广大中间商领域允许用户可以因为有价值的关注（通过浏览器的用户感兴趣的措施使其更有价值和更相关）而得到补偿的广泛领域的中间人，而不影响广告客户的成本，对发布商收入的积极影响。从财务角度来看，这可以看作是其他短期促销活动的一种变化：广告客户经常为产品提供优惠券和折扣。促销不能解决在第一个地方广告商的产品告知客户的问题。促销活动也不会减少用户忠诚或交易。大多数CMO同意通过促销可以改善短期销售，但通过促销无法实现可持续的竞争优势，所以需要使用广告。

5.2 三向交易的科斯模型

三向的科斯定理是经济学家们研究兴趣的一个来源。在某些情况下，“空心”的存在使科斯定理适用于涉及多个不同玩家的现实世界的例子受到质疑[26]。尽管在线广告市场中有三位以上的参与者，我们可以将他们理想化为三位参与者：广告客户，发布商和用户。这种分析有助于理解游戏理论性考虑，解决与提出科斯模型交易讨价还价的任何“空心”论证，以及说明出版业的可怕状态。

作为交换媒介，我们提出了一种密码安全代币基本注意力代币（BAT），以便于保护用户的隐私，从而促进了科斯模型的交易。

广告客户希望购买用户的注意力。这大体上类似于上文科斯定理的“生产成本”，我们遵循的原则。

广告客户以C_a^a 价格估值用户的注意力。发行人希望将注意力以C_a^p 向网站支付。观看网站的用户以对网站内容的注意力估值C_a^c。

目前生态系统中的广告商和出版商具有与注意力货币化相关的交易成本。广告客户因为提供用户的关注支付给发布商。本系统的中介人创造了成本，因此$C_a^p < C_a^a$.

请注意，当我们谈到科斯定理的“交易成本”时，我们提到科斯模型游戏的参与者之间谈判交易的交易成本，因此，相当尴尬的是，将广告发送给出版商的货币成本不被认为是“交易成本”本身。

目前的广告生态系统产生“社会成本”或注意力污染，正如我们上面讨论的那样。已知这些社会成本很大。对于大部分用户（广告行业的22%红外线状态），社会成本大于注意力成本。按照上述的例子，我们将把污染成本标注为P_a^c。在目前情况下，只要$C_a^c > P_a^c$，用户将会查看发布商和广告客户的内容。每个用户都是不同的，当然，发布商和广告客户也有所不同，但是$C_a^c < P_a^c$用户大量存在和增加表示我们正在接近这个不平等的时间。这个结果是$C_a^p = 0 \iff (C_a^c < P_a^c)$。

由于C_a^c 与发行商的利润成比例（以及广告客户在“注意力”中的利润），所以任何

价值保持在$C_a^c > P_a^c$ 对发布商和广告商都是有利的。在这个论点中，广告客户和发布商有效的联合在一起是个工厂，用户拥有污染权。但是，用户也会重视发布商的产品。在$C_a^c < P_a^c$ 的退化情况下，用户也因为注意力经济崩溃而最终受到伤害，而用户也占有其他兴趣。

社会成本应分解为其组成部分。我们已经确定了上述广告业博览会社会成本的主要组成部分。安全风险是一个组成部分，P^s。黑客网络可以将广告放置在不必要的广告交易平台中，对于个人用户以及展示这些广告的发布商来说，这可能会产生巨大的成本。

隐私损失是与目前存在的广告格局相关的非常重要的社会成本，P^p。广告商目前需要隐私入侵，以确保广告实际上被相关用户查看。实际上，广告商正在为增添价值到注意力付出代价。

数据成本也是当前广告生态系统的社会成本的重要组成部分，P^d。这些费用通常由用户为广告客户和出版商服务的中间商的活动承担。这些成本似乎是微不足道的，但是对于许多用户而言，它们是推动广告拦截器采用的主要原因。对于在线广告资源内容的所有观众，在处理下载和执行所有隐私违规代码的费用方面花费了相当长的时间。除了这笔费用外，对于那些使用移动设备的用户而言，货币收费很有意义。据估计，前50名新闻网站比向这些ads9的移动用户投放广告的数据费用的实际费用减少了16倍！由于发布商提供的数据的一半以上是与广告相关的，所以一半的数据计划可以每年上百美元直接用于移动用户。

最后，由广告本身产生的成本，P^a。在大多数情况下，这不是一个巨大的成本，但是广告主最重视的事情，应该单独考虑。如果广告可以相关，P^a 甚至可能是负面的。有些用户喜欢看某些广告。

所以，我们现在的在线广告生态系统的社会总成本是

$$P_a^c = P^a + P^d + P^p + P^s$$

对于给定的P^a值，这是广告客户实际估价的值，如果我们可以消除其他因素，则P_a^c 将始终较低。具有匿名功能的基于代币的系统将完全删除P^p。P^d不会被代币系统完全减轻，因为一些网络流量将发生在服务系统并呈现广告本身。由于只需要将几个字节的数据传输到服务代币，所以这个成本将仅在下载广告的内容中有效; 相当大的改善。使用加密协议和零知识证明，以及使用已知的发布商和广告商也会大大降低P^s。

所以，对于正确的隐私保护代币系统：

$$P_a^c(\mathrm{BAT}) = P^a + P^d_{\mathrm{BAT}} + P^s_{\mathrm{BAT}}$$

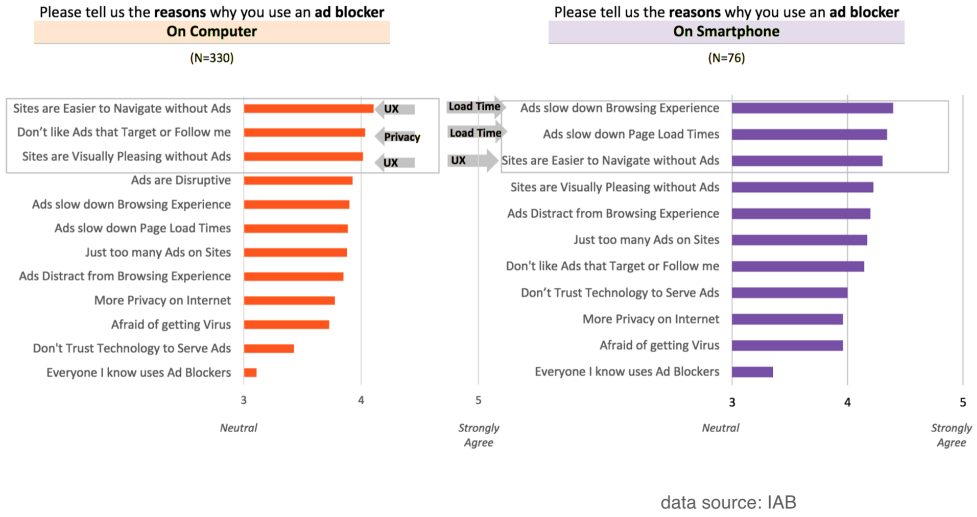


Figure 13: 阻止广告的主要原因：用户体验和隐私

为了接近第一阶段，

$$P_a^c(\text{BAT}) = P^a + P_{\text{BAT}}^d$$

剩下的社会成本可以通过支付可用于其他事物的用户补偿来减少或消除（例如，支付出版商的优质内容或与内容相关的应用程序）。在这里介绍的简化的游戏理论案例中，发布商最终会恢复广告支出的这一部分，因为发布商是唯一可以花费注意力代币的地方。在更广泛的情况下，用户可以在其他发布商处使用代币，发布商所收取的收入受用户收取的比例的限制。在提议的方案中，代币在广告活动中分配的方式，发布商接收的广告支出远远大于他们目前收到的广告支出的提议。

由于用户也收到对他有用的东西，我们可以安全地声明$P_a^c(\text{BAT})$ 为零或负数，这应鼓励用户查看更多的发布商内容。有些人可能会反对用户为了注意活动而获得的代币只能用在发行商的“公司商店”中，但是由于代币可能以不同的方式被保存和使用，所以它对用户有价值，就像航空公司提示要点和视频游戏代币。

广告客户在这个生态系统中为给定的关注度的支出应该更小，因为与提供所需注意事项相关的社会成本较少。此外，广告商并不需要为中间商支付社会成本来获得他们的广告内容被发送给相关用户的信心。由于这种情况对于发布商来说更好，并且使更快乐和更“富有成效”的用户、广告客户应该因为他们的广告支出而获得更多收益。

总而言之，我们使用科斯定理来证明使用BAT系统为浏览器用户、广告商和发行商在注意力经济中提供了更低的成本。广告客户将获得用户关注的优异份额，以及用户参与的有力证明。发布商将获得更大的广告收入份额。用户将获得相关广告和广告

收入份额的宝贵经验。

5.3 BAT的稳定性分析

荷兰经济学家von Oordt和Bolt在2016年介绍以假设虚拟货币汇率的模型[25]。该模型假设虚拟货币的价值由三个主要因素组成：虚拟货币付款的效用，前瞻性投机者对虚拟货币供应的决定以及推动用户采用和商家接受虚拟货币的因素。

这个论点源自费雪1911年的观察结果，投机者可能会有效地限制货币供应量，以期望更高的未来效用。由于这种动态特别适用于诸如比特币或BAT等有限发行的货币，它可能是虚拟货币的代币销售定价和稳定性分析的重要因素。

对于具有固定数量的货币代币MBAT的简单经济体系，可以记下交易量关系：

$$P_t^{\mathrm{BAT}} T_t^{\mathrm{BAT}} = M^{\mathrm{BAT}} V_t^{\mathrm{BAT}}$$

V_t^{BAT} 是BAT 的流动速度，在定义的时间段t内，每单位BAT 用于购买服务的平均次数。T_t^{BAT} 是在t期间购买的服务数量，P_t^{BAT} 是服务的加权价格。

插入以$为单位汇率

$$\frac{P_t^{\mathrm{BAT}}}{P_t^{\$}} T_t^{\mathrm{BAT}} = M^{\mathrm{BAT}} V_t^{\mathrm{BAT}}$$

由于我们可以假设传统的法定货币是所有相关方的会计单位，我们定义汇率为$S_t^{\frac{\$}{\mathrm{BAT}}}$，并用上面的方程式代替

$$S_t^{\frac{\$}{\mathrm{BAT}}} = \frac{T_t^{\mathrm{BAT}}}{M^{\mathrm{BAT}} V_t^{\mathrm{BAT}}}$$

如果我们考虑在服务转移中没有使用的货币数量，我们可以假设实际用于结算$\widehat{V_t^{\mathrm{BAT}}}$. 将$Z_t^{\mathrm{BAT}}$ 定义为事务中未使用的BAT单元的数量。

由于在我们经济中的整体速度V_t^{BAT} 是所使用的货币单位与未用于转让服务的单位之间的平均值，

$$V_t^{\mathrm{BAT}} = \frac{M^{\mathrm{BAT}} - Z_t^{\mathrm{BAT}}}{M^{\mathrm{BAT}}} \widehat{V_t^{\mathrm{BAT}}}$$

将这些融入汇率

$$S_t^{\frac{\$}{\mathrm{BAT}}} = \frac{\widehat{T_t^{\mathrm{BAT}}}}{(M^{\mathrm{BAT}} - Z_t^{\mathrm{BAT}}) \widehat{V_t^{\mathrm{BAT}}}} \tag{1}$$

因此，BAT代币的汇率与购买的服务量成正比，并且与时间段t 内交易中未使用的货币成反比。这个方程包含了流通中缺乏货币会导致汇率上升。

我们现在把注意力转向不用于交换的BAT的数量。一些Z_t^{BAT} 代币可能是用户忘记他们持有的少量代币的结果。有些可能是因为传统货币的交收延迟。总体而言，不交易的代币持有者在现代风险管理理论方面有标准的方法来评估代币的未来效用。

由于代币是无趣的，所以有一个折扣条款与在其中持有z_t^{BAT} 大小的位置相关联。

$$-RS^{\frac{\$}{\mathrm{BAT}}}z_t^{\mathrm{BAT}}$$

其中R 是在传统货币的利率折扣。

如果我们将BAT持有量的未来预期值视为BAT中未来预期价值的总和

$$||S^{\frac{\$}{\mathrm{BAT}}}t+1||z_t^{\mathrm{BAT}}$$

利用这个贴现利率期限（其中R 是贴现运营商），以及由风险厌恶项目γ计算的BAT未来位置的波动性，我们从现代投资组合理论到达了有效的前沿。

$$||S_{t+1}^{\frac{\$}{\mathrm{BAT}}}||z_t^{\mathrm{BAT}}-R(S_t^{\frac{\$}{\mathrm{BAT}}})z_t^{\mathrm{BAT}}+\gamma\sigma^2(||S_{t+1}^{\frac{\$}{\mathrm{BAT}}}||)z_t^{\mathrm{BAT}}=0$$

使用这个标准结果，我们可以在给定的时间段内解决个人持有的代币的最佳数量。

$$z_t^{\mathrm{BAT}}=\frac{||S_{t+1}^{\frac{\$}{\mathrm{BAT}}}||-R(S_t^{\frac{\$}{\mathrm{BAT}}})}{\gamma\sigma^2(||S_{t+1}^{\frac{\$}{\mathrm{BAT}}}||)}$$

如果我们考虑在给定时间间隔t内持有BAT的所有人员，我们将经济有效的获得BAT的数量供以后使用。

$$Z_t^{\mathrm{BAT}}=N_tz_t^{\mathrm{BAT}}=\frac{||S_{t+1}^{\frac{\$}{\mathrm{BAT}}}||z_t^{\mathrm{BAT}}-R(S_t^{\frac{\$}{\mathrm{BAT}}})}{\frac{\gamma}{N_t}\sigma^2(||S_{t+1}^{\frac{\$}{\mathrm{BAT}}}||)}$$

由于这个价值不能是负的，我们假设持有BAT的人有这样的立场

$$||S_{t+1}^{\frac{\$}{\mathrm{BAT}}}||\geq R(S_t^{\frac{\$}{\mathrm{BAT}}})$$

因此，利用我们上述的关系，我们得到BAT预期的未来价值，利率和BAT经济转移速度之间的关系：

$$R^{-1}(||S_{t+1}^{\frac{\$}{\mathrm{BAT}}}||)\geq\frac{T_t^{\mathrm{BAT}}}{M^{\mathrm{BAT}}V_t^{\mathrm{BAT}}}$$

因此，如果贴现的预期值超过当前汇率的假设值，人们将持有BAT。所以，汇率是BAT未来预期值的函数

$$S_t^{\frac{\$}{\mathrm{BAT}}} = R^{-1}(||S_{t+1}^{\frac{\$}{\mathrm{BAT}}}|| - \frac{\gamma}{N_t} Z_t^{\mathrm{BAT}} \sigma^2(||S_{t+1}^{\frac{\$}{\mathrm{BAT}}}||)) \tag{2}$$

因此，BAT持有量是预期未来汇率折现减去BAT未来价值不确定性的风险溢价。

如果模型成立，1 和2 可用于定义BAT的供应和需求。由于M^{BAT}在BAT的情况下不是依赖时间的，所以可以很容易地理解BAT交易和BAT交易未来效用的意见。随着BAT交易的增加，汇率变得由交易主导，而不是未来的效用预期。在成熟的虚拟货币以及各种其他内部代币系统中观察到这种动态。

虽然模型不精确，但这种模式认为在代币中介经济中长期价格稳定。

References

[1] T. H.; Beck J. C. Davenport. *The Attention Economy: Understanding the New Currency of Business*. Harvard Business School Press, 2001. ISBN: 978-1578514410.

[2] Wikipedia. *AIDA (marketing)*. [Online; accessed 22-January-2017]. 2017. URL: https://en.wikipedia.org/wiki/AIDA_(marketing).

[3] Jack Neff. "P&G Tells Digital to Clean Up, Lays Down New Rules for Agencies and Ad Tech to Get Paid". In: *Advertising Age* (Jan. 2017). URL: http://adage.com/article/media/p-g-s-pritchard-calls-digital-grow-up-new-rules/307742/.

[4] Paul Sholtz. "Transaction Costs and the Social Costs of Online Privacy". In: *First Monday* 6.5 (May 2001). URL: http://firstmonday.org/issues/issue6_5/sholtz/index.html.

[5] Lee Rainie. "The state of privacy in post-Snowden America". In: *Pew Research Center FactTank* (Sept. 2016). URL: http://www.pewresearch.org/fact-tank/2016/09/21/the-state-of-privacy-in-america/.

[6] Margaret Boland. *Cyber criminals are stealing billions from the ad industry each year*. [Online; accessed 22-January-2017]. 2016. URL: http://www.businessinsider.com/the-ad-fraud-report-bot-traffic-2016-3.

[7] Hillary Tuttle. "The Rise of Malvertising". In: *Risk Management Monitor* (Aug. 2015). URL: http://www.riskmanagementmonitor.com/the-rise-of-malvertising/.

[8] Rob Leathern. "Carriers are Making More From Mobile Ads than Publishers Are". In: *Medium* (Oct. 2015). URL: https://medium.com/@robleathern/carriers-are-making-more-from-mobile-ads-than-publishers-are-d5d3c0827b39\#.aiw3hs4ls.

[9] eMarketer. *US Ad Blocking to Jump by Double Digits This Year*. [Online; accessed 22-January-2017]. June 2016. URL: https://www.emarketer.com/Article/US-Ad-Blocking-Jump-by-Double-Digits-This-Year/1014111.

[10] Interactive Advertising Bureau. *Ad Blocking: Who Blocks Ads, Why and How to Win Them Back*. Tech. rep. Interactive Advertising Bureau, 2016. URL: http://www.iab.com/wp-content/uploads/2016/07/IAB-Ad-Blocking-2016-Who-Blocks-Ads-Why-and-How-to-Win-Them-Back.pdf.

[11] Mathew Ingram. "How Google and Facebook Have Taken Over the Digital Ad Industry". In: *Fortune* (Jan. 2017). URL: http://fortune.com/2017/01/04/google-facebook-ad-industry/.

[12] Mark Jurkowitz Amy Mitchell and Kenneth Olmstead. *Social, Search and Direct: Pathways to Digital News*. Tech. rep. Pew Research Center, Mar. 2014. URL: http://www.journalism.org/2014/03/13/social-search-direct/.

[13] Digital Content Next Research Team. *DCN' s Distributed Content Revenue Benchmark Report*. Tech. rep. Digital Content Next, Jan. 2017. URL: https://digitalcontentnext.org/blog/2017/01/25/dcns-distributed-content-revenue-benchmark-report/.

[14] YouExec. *Google & Facebook ad traffic is 90% useless*. [Online; accessed 22-January-2017]. Jan. 2017. URL: https://youexec.com/dev/2017/1/14/google-facebook-ads-traffic-is-useless.

[15] Chris Pemberton. *Gartner CMO Spend Survey 2016-2017 Shows Marketing Budgets Continue to Climb*. Tech. rep. Gartner Research, Dec. 2016. URL: https://www.gartner.com/smarterwithgartner/gartner-cmo-spend-survey-2016-2017-shows-marketing-budgets-continue-to-climb/.

[16] Jack Simpson. *40% of publishers describe their digital ad revenue as shrinking or static*. Tech. rep. Econsultancy, Oct. 2015. URL: https://econsultancy.com/blog/67028-40-of-publishers-describe-their-digital-ad-revenue-as-shrinking-or-static/.

[17] Dimitri DeFigueiredo. *Github discussion of concave score*. May 2016. URL: https://github.com/brave/ledger/issues/2#issuecomment-221752002.

[18] S. Myers R. Pass S. Hohenberger and A. Shelat. "An Overview of ANONIZE: A Large-Scale Anonymous Survey System". In: *IEEE Security and Privacy* 13.2 (2015), pp. 22–29.

[19] Abhi Shelat Rafael Pass. "Micropayments for Decentralized Currencies". In: *CCS '15: Proceedings of the 22Nd ACM SIGSAC Conference on Computer and Communications Security* (2015), pp. 207–218.

[20] Matthew D. Green Jingcheng Liu Ian Miers Peihan Miao Pratyush Mishra Alessandro Chiesa. "Decentralized Anonymous Micropayments". In: *EUROCRYPT 2017 (36th International Conference on the Theory and Applications of Cryptographic Techniques)* (2017).

[21] Ian Miers Matthew Green. "Bolt: Anonymous Payment Channels for Decentralized Currencies". In: *IACR Cryptology ePrint Archive 2016* (2016).

[22] Jens Groth. "Short pairing-based non-interactive zero-knowledge arguments". In: *Proceedings of the16th International Conference on the Theory and Application of Cryptology and Information Security,ASIACRYPT '10* (2010), pp. 321–340.

[23] Iddo Ben-Tov Alessandro Chiesa Ariel Gabizon Daniel Genkin Matan Hamilis Evgenya Pergament Michael Riabzev Mark Silberstein Eran Tromer Eli Ben-Sasson and Madars Virza. "Computational integrity with a public random string from quasi-linear PCPs". In: *EUROCRYPT 2017 (36th International Conference on the Theory and Applications of Cryptographic Techniques)* (2017).

[24] Reed Hundt. *Statement of Reed Hundt, Chairman of the Federal Communications Commission on Spectrum Policy Management before the Subcommittee on Telecommunications, Trade and user Protection, Committee on Commerce, U.S. House of Representatives*. Feb. 1997. URL: https://transition.fcc.gov/Speeches/Hundt/spreh743.html.

[25] Wilko Bolt and Maarten van Oordt. *On the Value of Virtual Currencies*. Tech. rep. Working Paper No. 2016-42. Bank of Canada, Apr. 2016.

D:20170508234544+08'00'