
XCHNG
BROUGHT TO YOU BY KOCHAVA

目录

XCHNG 摘要

数字广告始于1994年的首个横幅广告。[1]在接下来的几年中，这个新兴行业成为了以数字化方式接触受众的主要手段。如今，数字广告已是全球2240亿美元的成熟行业；[2]，美国的市场规模为830亿美元，其中580亿美元在移动端。[3]

无数的广告商、代理商、出版商、交易所、广告网络和联盟网络推动了数字广告业的发展。今天，该行业触及了网络、搜索、社交、移动、应用程序、跨屏和OTT服务等领域，还在试水VR（虚拟现实）、AR（增强现实）、交通工具端以及通过智能冰箱投放的广告。由于该行业的规模，提供支持的中间件也已发展壮大，发挥了“胶水”的作用，将数字广告的各个组成部分（例如，广告服务器、中介服务器、欺诈监控、归因和标签管理、创意管理、优化服务和分析提供商等）粘接在一起。

尽管增长迅猛，触达范围广，在该生态系统中交易的参与者众多，但该行业却在使用一种基于文件的过时合约框架，称为“广告订单” (Insertion Order，IO)，不仅效率低下，还缺乏核实合同承诺的机械化方式。此外，履行IO条款的次级参与者众多，再加上整个行业缺乏透明度，因此IO交付过程中存在大量进行欺诈的机会。

自1994年的HotWired广告以来，数字广告行业已经走过了一段漫长的道路，但运营在许多方面还停留在过去：

- 没有一个能够在保护目标受众设备真实身份的同时实现大规模受众定位的系统。缺少这样的系统导致该行业依赖于Google和Facebook广告双寡头。

> 今天，美国的数字广告业的规模已经达到830亿美元，其中580亿美元在移动端。[3]

- 每1美元支出中有50美分用在了中间件、中介和减少欺诈上。[4]
- 广告订单缺少交易和验证条款的自动化机制。

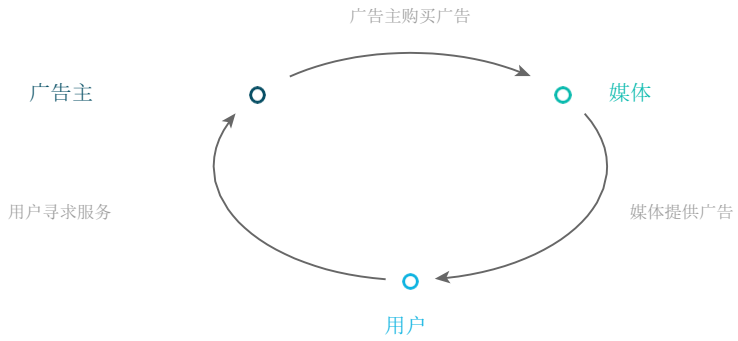
Kochava实验室SEZC正在推出XCHNG平台，为数字广告生态系统提供一个开放、统一的区块链框架，a) 通过智能合约IO构建广告买卖的工作流，b) 实现受众匹配和激活，c) 提高广告支出的效率和安全性，d) 采用下一代广告系统，为生态系统中的所有参与者提供记录，e) 对该框架实现代币化，将数字广告作为真正的资产类别。

1 https://www.wired.com/2010/10/1027hotwired-banner-ads/
2 https://www.emarketer.com/Report/Worldwide-Ad-Spending-eMarketer-Forecast-2017/2002019
3 https://www.emarketer.com/Report/US-Ad-Spending-eMarketer-Forecast-2017/2001998
4 Arete 广告技术概述：数字广告：以任何标准衡量均显疯狂的市场 —— 2017年5月22日

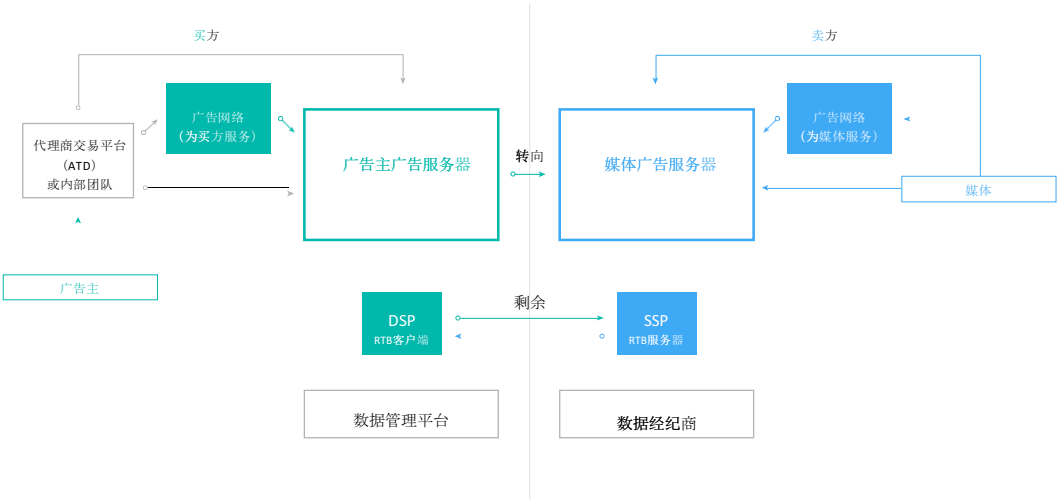
当今的数字广告

概况

数字广告最简单的形式是，通过互联网、移动应用和其他连接设备促进向消费者投送营销信息和内容。



实际上，这个过程已变得极其复杂，许多参与者在这个生态系统内按照各自的合约协议进行合作。



当前数字广告生态系统运作方式示例

买方/广告主

买方或广告主（也称“营销商”）购买媒介，为其应用、游戏、服务、创意、网站或产品做数字广告。

媒体

媒体（公司或个人）是一个拥有已发布网站或应用程序的实体，能向其受众展示广告。这些广告通常由广告主提供，目的是向相关媒体的受众推销产品、服务或应用。媒体提供一定数量用于展示广告的单元（横幅广告、视频广告、插页式广告、内容广告或其他一些特别的单元类型）。就本白皮书而言，我们将广告单元称为广告位。一个网页或应用可能有一个或多个部分的广告位，用于展示各种格式的广告。

聚合平台

为了支持一个典型的广告活动（也称为"广告购买"）所需的广告曝光量，广告主可能会使用多个媒体实现活动目标（即，获得充足的广告位）。广告主还可能与任意数量的广告网络（也称为"供应方提供商"，supply-side provider，SSP）接洽，这些广告网络聚合了众多媒体提供的广告位，以便广告主更大规模地购买覆盖更大受众群体的广告位。同样，一个拥有多个广告位的媒体可以与多个广告主合作，填充广告位。相反地，这些媒体也可与广告主聚合平台（也称"需求方提供商"，demand-side provider，DSP）合作。广告主聚合平台聚合了众多广告主的广告，可填充可用的广告位。此外，SSP也与DSP交互，以提供更大的规模经济。目前，这种聚合系统完全是中心化的。

过程

IO的谈判以及按照规则执行所需的管理工作是一个冗长乏味的人工过程，而致力于促进规模的第三方合作伙伴（SSP和DSP）的参与使得这项工作更加复杂。购买或出售广告位的过程需要以下工作：

- 针对每个活动（或排期）签署IO（用于提交交易的合约）
- 确定详细的付款条件
- 对相关排期的过滤和定位标准进行量化（根据广告购买确定相对应的受众特征）
- 除上述之外，广告主通常会规定补充条款，其中包括：
  - 每日投放排期 (Daily Pacing)：媒体不是一次性地在一个广告位中展示广告，而是按规定的时间安排展示
  - 填充保证：媒体根据广告库存量的变化履行IO

定价

媒体和SSP作为一方，而广告主和DSP作为另一方，依靠一对一的谈判签署IO。历史上，针对每个广告源的广告库存价值建立了价目表，目前则是媒体和SSP根据定位标准使用很高的折扣和溢价。这些定位标准包括以下全部要素：一天中的时间段、
网络随机与具体网站定位、地理位置定位、网页或应用上的广告位位置、广告位类型、广告位供应、对广告的需求等。

难以对广告库存确定准确的市场价值会对需求方和供应方造成不利影响。常见的真实市场情况是，媒体往往低估库存价值，而广告主常常可能为所需库存过多地付款。

广告主通常会为在广告位中展示广告支付一定的价格。在广告位中投放广告或其他数字内容或媒体称为展示 (impression)。通常，广告主会根据预期的投资回报（例如，网页或应用的用户购买广告中展示的产品）为每次广告展示向媒体支付价格。导致广告观看者做出某种行动的展示被称为转化。应指出的是，转化不限于购买产品，还可包括观看者点击广告中的超链接以获取相关产品的更多信息。

如上所述，数字广告市场可包括供应方经济体和需求方经济体。需求方经济体包括广告主（或DSP），需要展示库存用于在广告位中投放广告。供应方经济体包括媒体（或SSP），提供展示库存用于在广告位中投放广告。随着媒体SSP数量的增加，可供广告主或DSP购买的可用展示数量也在相应地增加。在传统市场中，实时竞价 (RTB) 可用于向广告主出售可用展示。RTB框架的一个实现示例是OpenRTB，这在美国互动广告局 (Interactive Advertising Bureau) 的《OpenRTB API规范》版本2.3.1中有详细的描述[5]。

无论是否使用OpenRTB，所有的RTB实现都使用中心化客户端服务器竞价的相同基本框架。RTB使SSP能够向媒体获取展示库存并以市场竞价方式出售给DSP。在该场景中，SSP聚合了展示的供应，而DSP聚合了广告投放的展示需求。SSP和DSP共同形成了拍卖式市场。通常情况下，RTB环境中多个买家出价竞买每个展示（基于每次展示）。买家通常是DSP，但大型广告主也可能进入RTB市场。通常，设立RTB市场是为了将标的授给出价达到或高于第二高竞价者的竞价者。最后，RTB通常作为最后的努力，销售未作为优质库存出售且被归类为剩余的那些库存。

鉴于当前数字广告生态系统的复杂性和无效性，再加上双寡头的统治，建立新范式的时机已经成熟。

RTB以及DSP和SSP在买卖展示中扮演的角色可视为克服上述挑战的一种手段。这种方法的问题在于仍然存在中心化的要求，即特定的DSP必须与可用的SSP相连接。同样，对于向买家提供库存的媒体，聚合的SSP必须与向他们购买库存的DSP相连接。在大多数情况下，广告主仍须咨询并使用多个DSP，这既复杂、低效，又昂贵、耗时。同时，另一个担忧是，如果广告主与多个DSP合作，而这些DSP都连接相同的SSP，广告主实际上会与自己竞争。（在这种情况下，同一个广告主通过两个独立的DSP推高了自己的成本）。

5 美国互动广告局。《OpenRTB API规范》版本2.3.1。Accessed July 7, 2017. https://www.iab.com/wp-content/uploads/2015/06/OpenRTB-API-Specification-Version-2-3.pdf.

DSP可能也签订IO，然后直接向特定的媒体购买库存。对此，广告主可能知道也可能不知道。同样，收到子订单的媒体可能转而向第三方媒体购买来履行IO。这就会造成多级代理的情况，而这种情况在真正的市场驱动的环境中既没有被追踪，也没有说明。

最后，由于RTB只能提供立即可用的库存，因此没有办法为未来的广告购买解决基于拍卖的市场变动问题。

随着可用展示数量的不断增加，广告主、媒体和相关供应链在管理展示的供需方面面临越来越高的复杂度，即确保快速、高效地向需要投放广告的广告主出售可用的展示，并且以开放、分散化的方式进行出售。

数字广告的测量

数字广告生态系统中的测量涉及测量展示次数、点击次数、关键绩效指标（体现推广工作的转化率），以及评估消费者和源媒体的终生价值 (lifetime value, LTV)，以指明广告主是否应购买更多的相关库存。独立于广告主和媒体的测量方（真正独立的第三方）通常最值得信赖，这就要求1.) 被广告主采用作为单一的记录系统，2.) 得到库存源媒体的信任并将测量工具进行集成。

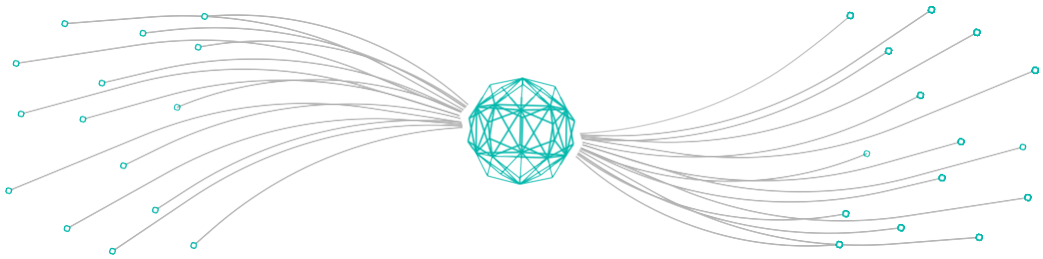
随着可得展示数量的增加，广告主、媒体和相关供应链面临的复杂程度也越来越高。

在网络上，以前的测量方式是跟踪媒体活动（展示和点击），并另行测量指定网络财产上的像素，从而确定关键绩效指标 (KPI)。移动端的情况更加复杂，需要一个集成的软件开发工具包 (SDK) 来跟踪移动应用的KPI。在Web 1.0的年代，DoubleClick是测量方面的主要领导者。在Google收购DoubleClick之后，市场出现了其他独立的工具（如Adometry和Convertro，这两家公司都已被收购）。

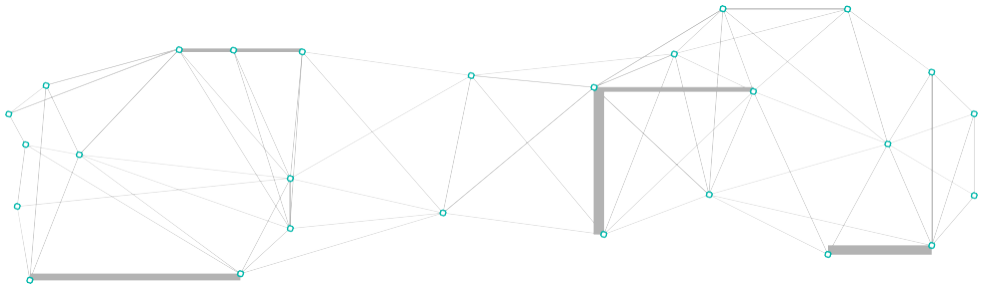
明天的数字广告：

促成端到端工作流的全球分布式账本

需要一种通过基于加密的分布式账本促成IO交易的替代技术方法。这种统一、开放的方法将使参与IO工作流的各方能够一起交易。这一切从发现和谈判开始，覆盖包括执行、测量、付款和参与者评定的整个生命周期。



广告主　　当前的中心化系统　　受众



开放的去中心化框架

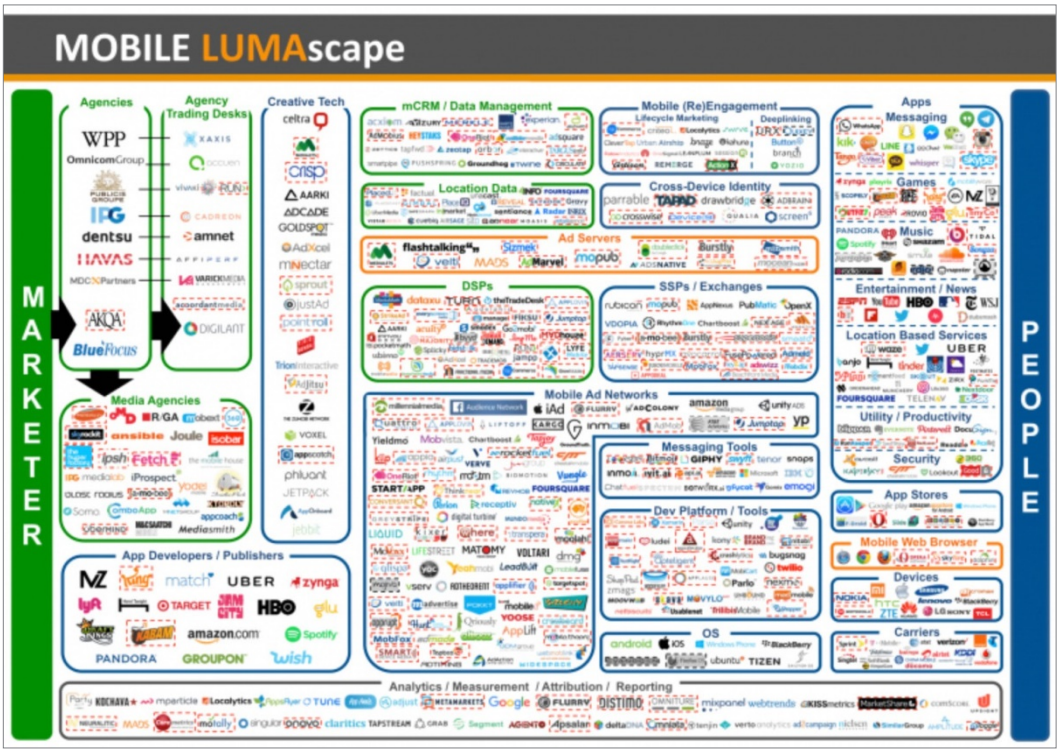
基于2015年申请的专利，Kochava对于这样一种系统拥有专属权利。其框架基于普通的李嘉图合约 (Ricardian contract) 与一个名为XCHNG的开放式区块链实现，能存留交易历史并在IO生命周期中提供最大限度提高效率所需的辅助实用程序。

通过该框架，一个商业实体（如Kochava Inc.）能够将其可证明的领导地位作为可靠的记录系统附在一个开放式区块链实现上，从而使生态系统进一步统一和扩展。该系统设想了一个应对数字广告运营现实的下一代区块链实现，并支持生态系统的必要组件从其当前状态不断发展。该系统旨在为参与者提供一个简单的路线图，以在数字广告开放式区块链标准上运行。现状是采用中心化的交换方式，而XCHNG框架是一种去中心化的方式。

尽管已有一些在数字广告方面利用区块链协议的技术（例如，adToken、Basic Attention Token、AdEx），但这些技术都没有提供端到端的解决方案，而且业内没有一家具有与Kochava Inc.同等业务范围和经验的公司认可将其中的任何技术可作为记录系统。尽管上述每种区块链技术都可与XCHNG交互，但必须指出的是，这些技术并没有试图达成XCHNG提出的目标。

很多行业为了保持生存力曾经进行了大幅改造，数字广告达到了与这些行业类似的“沸点”。例如：19世纪铁路行业经历了高速增长，各种独立的公司形成了自己的铁路网络，但在最初，轨距等细节问题却没有进行标准化，它们没有预料到设备最终需要交换。只有在铁路网络必须互连时，人们才得出深刻的观察，即共轨对于大规模的网络运输至关重要。当时，由于货物运输对国家利益极为重要，因此关于轨距的辩论逐渐形成了规范的标准。

同样，从1994年HotWired上的单个广告单元以来，现在的数字广告已经发展成了2,240亿美元的全球行业，拥有大量供应商，如果在张图上展示出来，看上去就像是一张视力表。该行业令人目眩，被价值主张所分化，正如以下LUMAscape的图所显示的。



XCHNG框架代表了一组通用、开放、可扩展的“铁轨”，在该框架上，Kochava等公司（以及上图中的参与者）可将区块链用于自身的商业产品。

Kochava Inc.承诺部署XCHNG并成为XCHNG系统的首个参考实现实例，从而为已与Kochava Inc.建立合作的价值链上的广告主、媒体和所有广告供应商提供更多的福利。正如业内的各种参与者所强调的，如果没有因素刺激现有工具平台大规模地应用技术并为此提供支持，获得广泛的采用会是一个巨大的挑战。

数字广告双寡头经营自己的市场，导致效率低下，获取了大部分的增长份额

并非所有人都相信开放式轨道框架对数字广告业有用。今天，Google和Facebook形成了双寡头。这两家公司一直努力使广告主能够轻易、方便、灵活地做广告，但代价却是难以形成真正开放的市场。因此，也造成了无法无摩擦、高效地使买卖双方合为一体。毫无疑问，这两家公司的方法取得了成功。根据美国互动广告局 (IAB) 的数据，2017年第一季度美国广告业务同比增长37亿美元，Facebook和Google占了增长份额的98%。尽管有这样的成功，但这并不是真正开放、透明、市场驱动的交易交换。

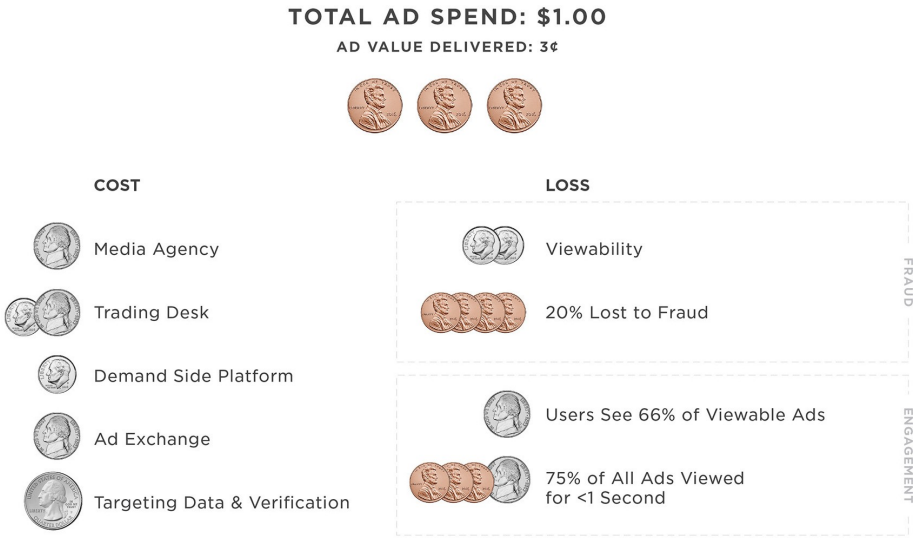
以下表格以上市公司作为真实开放市场的参考范例，显示了Google如何用自己的市场获取更多的广告收入并伪装成开放的市场。

交易所	做市商/IDB	经纪商	股票/财产
纽交所/伦敦证交所	投资银行	银行、Schwab、eTrade等	个股、综合指数、标普500等
Google AdX（10%费用）	DoubleClick (20%)	DoubleClick for Publishers (20%)	搜索、YouTube、地图、AdMob 等财产
Facebook数据管理平台 (Audience Manager)/Atlas	Facebook拍卖引擎/Atlas	Facebook受众网络 (Facebook Audience Network，FAN)	Facebook或FAN网站

Google以费用形式抽取了数字广告全部交易价值的30%-50%，还抓取了供应链中的数据，表示其为广告主提供了“基于市场的可用库存”。由于集成规则，Google占据了不成比例的市场份额。通过与金融市场的交叉比较，以下观察很清楚：

- **交易所不允许对单个股票/财产“坐庄”。**Google的情况是，它拥有自有财产的流动资金池，并经由AdMob通过第三方财产进行补充。Facebook的Facebook受众网络 (FAN) 也是如此。
- **做市商不允许对自己的股票提供流动性，因为这会导致市场操纵。**作为财产所有者，Google和Facebook可以看到“交易的双方”。
- **使Google成为YouTube的唯一经纪商（通过DoubleClick）并不是一个可行的市场条件。**尽管如此，凭借关联平台的优势，双方都设定了自己的规则。

在双寡头之外，使用独立参与者的效率并不令人印象深刻（这就是双寡头成功的原因）。这是因为广告主必须发现库存，确定条款，通过各种渠道购买广告，确保相关库存不存在欺诈，还需验证投放是否执行。此外，广告主还须大规模地完成上述各项工作，从而使其广告获得市场意义，能够触达绝大多数客户。



在目前的数字广告范式中，广告支出非常低效。

在存在双寡头的情况下，独立的媒体源和广告网络希望直接连接市场需求。

将数字广告转化为资产类别

资产类别是一组具有类似特征，在市场上表现类似，并且遵循一套共同的法律和法规的资产。金融业普遍认可现有3-5种核心制度性资产类别：[6]

- 证券（股票）
- 债券
- 房地产
- 大宗商品
- 现金（或现金等价物）

如前所述，对一个数字广告的买方和卖方具有约束力的合同通常采用广告订单（IO）的形式。为了规范IO的条款，美国互动广告局（IAB）为买卖双方建立了标准IO模板，以确保公平性和明确性。当前的版本是3.0.7[7]。一直以来，IO都是基于纸质文件或纸质文件的电子版，是具有约束力的合同，确定了有广告库存的媒体将向有意购买广告的广告主提供库存。随着价值链上参与者的分化，套利和多级代理已司空见惯，都将广告购买承诺作为了待交易资产的基础。

6 https://en.wikipedia.org/wiki/Alternative_asset
7 https://www.iab.com/wp-content/uploads/2015/06/IAB_4As_tsandcs_Education_FINAL.pdf

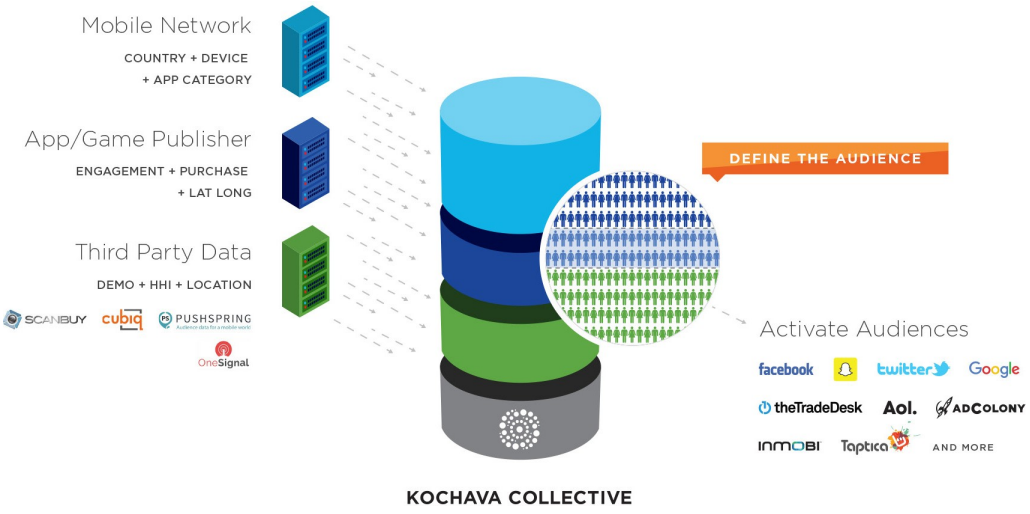
真正的资产类别将提供标准化的、完全集成的、可验证的数字广告库存，以及共同的流动性框架。

尽管代理商平台、交易平台和广告网络的行为就像在买卖、交易广告库存一样，但事实上没有一个做到了可以规模化的机械化。作为一种资产类别，数字广告很难规模化地进行验证，整个系统的集成效率非常低，而且没有共同的底层机制来提供流动性。

股票、债券、房地产、大宗商品和现金是流动性最强的资产类别，因此也是报价最多的资产类别。还有其他资产类别，如不动产、艺术品和收藏品等。一般而言，投资品的可选项越多，流动性越低。在当前状况下，买家与媒体之间已购买的IO不具有流动性，被视为已提供的服务（即向媒体的受众展示的广告）。将数字广告作为真正的资产类别意味着要提供标准化的、完全集成的、可验证的数字广告库存，以及共同的流动性框架。

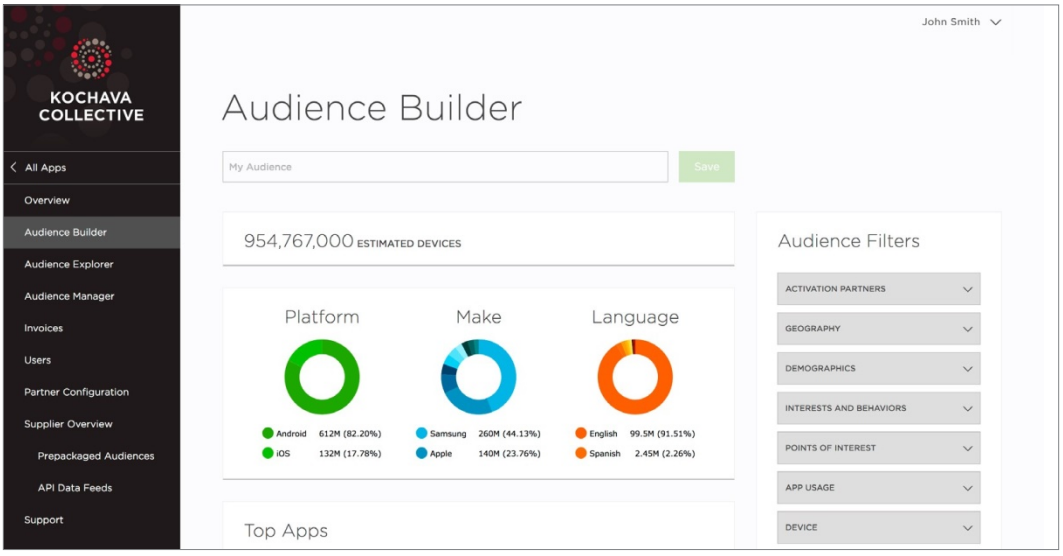
促成跨媒体源的开放式受众定位

2015年9月，Kochava Inc.为移动受众创建了一个名为Kochava Collective的新定位平台。Kochava Collective的基础是提供一个统一的受众图，使广告主能够为其广告活动查询和定位受众，并在设备一级达到精准。基于定位，该中心化系统将以去重复化的方式启用分布式激活，从而通过定位过程最好地寻找已识别的受众（即向已识别的受众提供广告）。

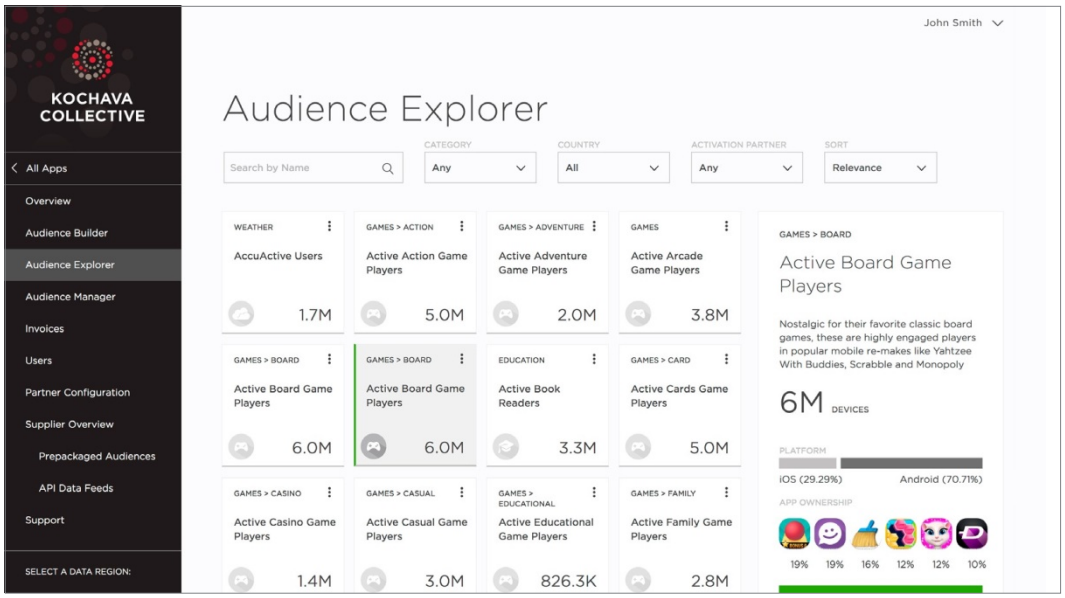


今天，Kochava Collective是一个中心化的移动设备数据库。Kochava Inc.在推出Kochava Collective时，着眼于为所有数字广告建立由区块链支持的记录系统，公司认识到这一区块链的价值将直接取决于广告主针对目标受众浏览该区块链的能力。

Kochava Collective上的客户概况屏幕示例



客户可在Kochava Collective中建立自定义受众或浏览符合其标准的预定义受众。



预定义受众可按类别、地理位置和激活合作伙伴进行搜索。

Kochava Collective已经获得了巨大的关注，成为了全球最大的独立移动数据市场（发布时有18亿唯一设备配置文件）。除了Google或Facebook外，其他工具平台都不能以相同的规模和精准度提供针对移动设备的目标定位能力。将Kochava Collective并入XCHNG区块链会为广告主提供一个重要且独有的机会。

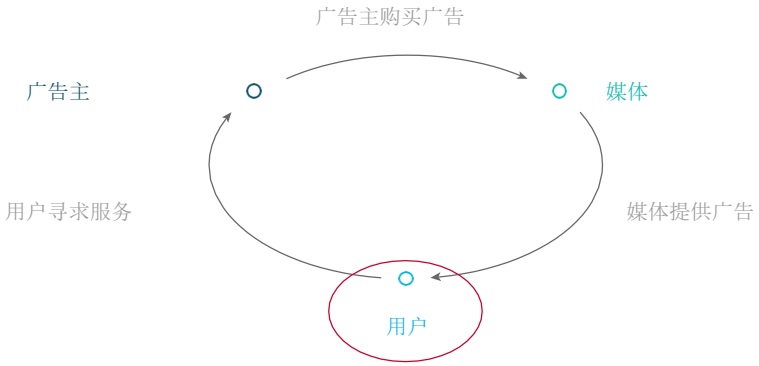
除了为广告主提供随意检索受众的能力外，Kochava Collective还提供了符合广告主挑选兴趣的预定义细分组。

虽然目前Kochava Collective是作为一个中心化的系统而建立，未来在XCHNG发布后，该系统将有能力使用媒体在XCHNG分布式系统上的输入的信息来丰富其数据。

这种方法将在向Kochava Collective的对手提供公开竞争机会的同时，促成XCHNG在整个行业的广泛采用。发布后，Kochava Collective将成为第一个使用XCHNG系统的目标定位工具平台参考实现实例，同时也是一个巧妙的行业竞争性用户界面，可用于发现并浏览在XCHNG上定位并激活的受众群体。

在数字广告的价值交换中发挥最终用户的作用

尽管广告价值链包括广告主、媒体和最终用户，但最终用户往往被排除在外。许多人认为，最终用户希望更好的兴趣匹配（也就是目标定位）以获得正确的推荐，并且广告能为他们带来收益。



XCHNG为最终用户创造了一种提交兴趣匹配标准的方式，供广告主在定位受众时使用。Facebook建立了良性的循环，即最终用户填写自己的兴趣，通过帖子进行参与，自行确认朋友，所有这些都被Facebook用作广告主定位标准。与此类似，XCHNG框架能使用户从匹配（定位）标准中获得价值。

XCHNG代币
和对未来的建议

Kochava设计并开发了一个开放的、基于加密的账本框架，这是广告业智能合约系统的表现形式。与基于纸质文件的数字广告买卖合同不同，智能合约IO将正规格式的IO中的所有元素编入完全可追踪且不可更改的电子李嘉图合约，对以下要件进行约束：

1. 根据开放式区块链框架，以相关目标定位能力识别并预先验证正在购买、出售或交易的库存
2. 使用唯一的密钥识别并预先验证媒介的买方和卖方
3. 协议的嵌入式和可编程条款，涉及流量和品牌安全验证、定位（基于上述第1项）、是否允许多级代理、排期时间、付款方式：CPM（按千次付费——基于展示的定价）、CPC（按点击付费）、CPI（按安装付费）、CPX/CPA（按行动付费）以及数字广告购买的其他详细规定；一般数据保护法规（GDPR）的合规规定
4. 确定负责测量IO条款绩效的生态系统相关合作伙伴（称为"测量服务商"）
5. 确定作为评级服务商的可选生态系统相关合作伙伴
6. 确定作为支付服务商的可选生态系统相关合作伙伴（为了清楚起见，Kochava不会在XCHNG上以此身份提供服务）。
7. 确定当买方、卖方或测量服务商在交付后存在分歧时，提供仲裁服务的可选生态系统相关合作伙伴

通过将IO编成智能合约，写入XCHNG分布式账本，相关库存实际上成为了一个资产类别，其中包含a) 可追溯的历史记录，b) 交付验证能力，c) 套利机会，以及最重要的d) 流动性。

XCHNG：用于广告业的区块链
要素的具体化能够实现利用支持性的不可更改基础设施对IO进行代币化，促成广告业中的各种参与者以商业化的方式进行参与。

XCHNG系统是一个全球分布式账本，可帮助买家和卖家与测量服务商、评级服务商和支付服务商进行交易，参与智能合约。XCHNG系统提供了各种技术方法，这使XCHNG系统具有差异性，并使整个系统在各垂直领域实现更快速的增长。其中一些差异化功能包括：

- **每日滚动链**
- **促进库存可寻址性的激励框架**
- **基于加密的激活；**在公开发布可寻址身份的同时保护身份
- **面向做市商的联合开放框架**

每日滚动链

区块链相关技术注重开放和透明的内在价值，往往针对链上记录的所有交易的完整历史记录，将此作为不可篡改性和匿名化透明度背后的基础。尽管这确实有价值，但在许多情况下，了解交易历史对于参与公司而言是一种竞争优势。例如，买家可能不希望详细地提供交易性购买历史记录（尽管会使用加密钥匙来代表一个参与者以实现匿名化）。此外，由于所有交易的完整历史链包含自第一天起的所有交易，因此这种架构会给链上的参与节点造成不必要的负担。事实上，在一些行业（如数字广告业），鉴于交易量，在链上存储每笔交易的标准做法会成为负担而非利益。

每日滚动链 (DRC) 可实现XCHNG的差异化并解决交易量方面的挑战。

基于这些原因，XCHNG系统提供了每日滚动链 (Daily Rolling Chain，DRC)。这是XCHNG区块链的一个关键特征和区别因素。其前提是，网络上的每个节点只保留并且只能验证给定日期的未完成合约的每日交易历史并向前推进。

区块链上排期已完成的合约都将不再同步，尽管这些合约的存在对整个区块链的签名有影响。总之，每一天都将是该区块链的第一天，而原区块会成为前一天交易的最后一个共识区块，区块链验证情况将根据参与共识的各节点的充分评级状态，在滚动时进行检查。

尽管任何节点都可以存储历史数据，但该系统架构的前提是，任何节点都不负责一天之外的任何数据。目前已有重大创新来实现DRC方法，同时还能确保对使用区块链评级系统的具体节点的信任，如此，新节点能够在同步每日滚动链时确信自己同步的是一个真实、正确的版本。

尽管DRC是开放系统的架构，但供应链中的主要供应商还是能够根据需要累积存储每天的交易，以确保自身为生态系统提供的商业服务。例如，像Kochava Inc.这样的测量服务商将存储单日以上的交易值作为测量服务商的一项服务。

虽然任何人都可以“收听”区块链并随着时间完整地存储一切数据，但我们认为只有那些提供服务的公司才会这样做，而不提供服务的公司则不会。此外，相比于早期采用的供应商，晚入的供应商由于少了在收听区块链之前的历史数据会面临“晚入市场”的后果。这为那些早期采用XCHNG系统向生态系统提供服务的公司提供了内在价值，而晚到的则享受不到。这就为新辅助参与者提供了激励，鼓励他们存储完整的历史链，作为对XCHNG系统新用户的服务。

总之，尽管在XCHNG的开放式区块链系统上展示交易历史提供了适当的透明度和开放性，但该系统的架构设计旨在避免系统上无关节点的不必要负担，并最大限度地扩展广告等高交易量应用的规模。

P2P网络

XCHNG网络是一个由对等 (P2P) 传输层组成的分布式网络。如果网络参与者共享自身的一部分硬件资源（例如，处理能力、存储、网络带宽等），则分布式网络可被视为P2P网络。每个网络参与者，或称作对等点 (peer)，可被其他对等点直接访问，无需经过中间实体。

对等点成员列表

分布式系统由一组需要通过彼此之间发送消息进行通信的节点组成。为了进行有效的沟通，各对等点必须能够识别网络中的其他对等点。每个对等点通常会维护自己能在网络中访问到的对等点的列表。随着更多对等点加入网络，维护该列表的整体复杂性也会增加。现已开发成员协议来帮助跟踪网络中的对等节点。一些成员协议依靠向对等点列表中的每个对等点发送“空心跳消息”来证实该对等点还“活着”。例如：

```
n = a remote node
t = random epoch time
for t
  r = send(heartbeat,n)
    if r != nil
      n = alive
    else
      n = dead
```

如果一个对等节点在一段时间后没有收到网络中另一个对等节点的心跳，则认为该节点已经“死亡”。对于一个小群体，这是可以接受的；但是，随着网络的增长，发送给列表中每个对等点的心跳消息数量会急剧增加。心跳协议解决了两个独立的问题：节点故障和维护网络中存活对等点列表的需要。

为了解决与P2P相关的网络限制，出现了基于gossip的成员传输协议。这些协议能减少每个对等节点发送的心跳消息数量。每个对等点都需将消息转发给网络中一组随机选择的对等点，而不是将消息直接发送给成员列表中的每个对等点。可扩展弱一致性传染风格进程组成员协议 (Scalable Weakly-consistent Infection-style Process Group Membership Protocol，SWIM)[8]等方法允许网络中对等点的弱一致性视图。这意味着给定对等点的成员列表最终会趋于与网络中其他对等节点相同的状态。SWIM方法由两部分组成：故障检测器和传播组件。故障检测通过随机探测对等节点完成：如果对等节点未能在给定时间窗口内确认消息，则尝试间接探测。间接探测选择多个随机对等节点来探测相关节点。间接探测可用于规避导致原节点探测失败的网络问题。如果间接探测失败，那么目标节点被标记为"可疑"。被标记为可疑的对等节点在设定的时间段内仍然是群集的成员。如果对等节点不能对网络的怀疑提出争辩，最终会被删除。在检测到一个对等点故障后，该对等节点只是向其余的存活对等点广播故障消息。收到此消息的对等点将从成员列表中删除故障对等点。发送成员消息的过程构成了传播组件。

此外，Kademlia[9]等方法使用分布式哈希表存储网络中的对等节点。Kademlia对等节点使用用户数据协议 (User Data Protocol，UDP）相互通信。节点ID可以识别每个对等节点。Kademlia算法用于查询在执行查找时最近的节点，只与系统中n个节点中的O(log(n))个节点联系。使用两个节点ID之间的异或（XOR) 操作作为节点之间的距离。Kademlia协议包括四个远程过程调用 (remote procedure call，RPC)：ping、store、find_node和find_value。ping RPC向一个对等节点发送探测，查看该节点是否在线。store RPC通知对等节点存储键值对供稍后检索。find_node RPC返回所提供的键值(key)对应的IP地址、UDP端口和节点ID。Find_value的作用与find_node RPC类似，不同的是，如果已对相关ID调用store RPC，则会返回存储的值 (value)。

XCHNG P2P网络中的对等点使用类似的协议。目前正在XCHNG中就性能、一致性和容错性测试类似于上述方法的策略。我们的目标是拥有可靠的、可扩展的、可容错的成员协议，在与网络中的对等点进行通信时，可为我们的P2P传输层使用。

消息广播

对等点从自己的成员列表中选择对等点来广播消息。P2P传输层仅负责传递消息。但是，为了帮助成功交付，还添加了额外的监控指标支持，例如往返时间 (Round Trip Times，RTT)、节点运行状况和其他常用指标等。传输层使用传输控制协议 (transmission control protocol，TCP)之上的双向流式传输来有效地向其他远程对等节点发送消息。每个对等点都有远程对等点的成员列表。当消息发送给一个对等点时，它们就开始向自己的远程对等点广播。

8 https://www.cs.cornell.edu/~asdas/research/dsn02-swim.pdf

9 https://pdos.csail.mit.edu/~petar/papers/maymounkov-kademlia-lncs.pdf

激励措施

为了获得成功，XCHNG系统必须像其他交易平台的实现性技术栈一样运作，激励供需双方参与系统。如果没有宝贵的供应，交易平台上就不会产生需求。同样，如果没有需求承诺，供应商也没有动力提供库存。

对于买家来说，激励效率、承诺库存量以及交易透明度都是充分的购买激励（假设工作流相对无摩擦）。也需为卖家（媒体）提供激励，促使它们在区块链上提供库存，还需进一步让数据提供者发布关于XCHNG批准库存的数据，以便能够正确定位。

在XCHNG系统上，矿工可以挖掘链上的各个区块，从而确保向买方提供的库存的质量和数量。此外，为了形成健康、内隐性的生态系统，矿工可写入关于在链上发现的交易的评级区块。评级会被用作链上参与者的相关元数据。

XCHNG系统将包含一个激励框架，以激励供应和数据合作伙伴在链上提供库存。该框架可能基于以下逻辑：

- 任何节点都可将可寻址受众的库存作为未经验证的库存引入XCHNG。可寻址库存指的是能够将广告投放到区块中指定设备的库存。包含在未经验证的库存中的是可寻址媒体源使用的可寻址标识符 (Cookie ID、IDFA、ADID)，如果这在生成的智能合约IO中提及，则广告必须按照该标识符进行投放。该标识符使用引入该库存的节点的键进行哈希，从而使得最终用户的广告标识符具有私密性，并且仅对由引入该库存的节点投放广告有效。
- 任何节点都可将有关可寻址受众的元数据作为未经验证的库存引入XCHNG。元数据包括但不限于设备特征、设备上运行的应用、地理位置数据或可用于目标定位的其他数据。元数据的主键是设备标识符（使用提供者的键进行哈希）。
- 测量服务商将交易写回智能合约IO，验证提供者引入的库存。

此外，XCHNG系统中的矿工可通过生成新区块来赚取代币。这些区块包括智能合约IO生成的交易。

通过密钥发布库存和激活受众

如前所述，XCHNG上的媒体将其库存作为未经验证的交易在链上提供。实际的广告设备标识符永远不会公开发布——所有标识符都用发布节点的键进行哈希。当买方定位XCHNG上智能合约IO中的受众时，已定位设备的标识符不会包含在合约的有效负载中。相反，所定位的或是非特定的设备定位数据，或是（在设备定位的情况下）未经验证的库存或经验证的库存。这种关联意味着媒体知道在XCHNG上签订的IO中要定位哪些设备，而其他节点不会知道IO中设备的身份。

与社区一致，XCHNG系统将有广告服务器和中介服务器的开放式实现，可自动将库存发布到链上，并自动集合未完成IO（以及相关的经过哈希的标识符）涉及的展示，以便媒体更容易采用。此外，XCHNG系统将采用一系列开放式插件技术，使得使用常用广告服务器技术（如DoubleClick for Publishers，DFP）做数字广告的媒体能够利用XCHNG系统上生成的需求。

面向做市商的联合开放设施

尽管XCHNG系统为买家和卖家优化，方便其直接买卖库存，但我们认为今天的广告业中还存在与股市中的做市商非常相似的重要角色。

在股市中，做市商通过显示对保证数量的股票的买入和卖出报价来争夺客户订单流量。做市商愿意购买证券的价格与公司愿意出售的价格之间的差额称为做市商价差。由于每个做市商都可以在任何特定时间买入或卖出股票，因此买卖价差就是做市商在每笔交易中的利润。做市商在收到订单后，立即从自己的持仓中出售股票或是寻找相抵的订单。根据日均交易量的不同，一只特定的股票可能会有多家做市商。做市商在二级市场中扮演着重要角色，特别在提高股票流动性方面，也因此促进了市场的长期增长。

同样，XCHNG系统为联合做市商提供了一种手段。不是提供股票进行买入/卖出，而是管理用于投放广告的各种财产。

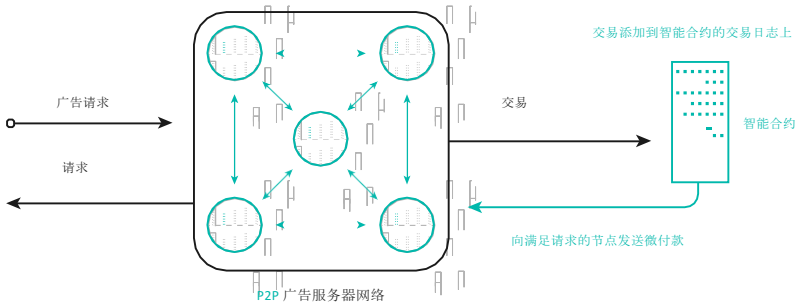
去中心化的广告投放矿工

XCHNG系统将智能合约IO通过gossip[10]方式传送给广告服务矿工的P2P网络。广告投放矿工通过提供自己的网络带宽和系统资源来履行广告订单。

矿工收到客户端请求并努力满足。投放成功后，客户端将收据发给矿工。矿工将收据发回XCHNG系统的IO以接收交易付款。对矿工的选择很大程度上取决于他们对请求的响应时间。但是，广告投放矿工也可能必须直接登录IO。如果矿工无法对客户端做出响应，则可使用传统的广告技术栈满足请求。

10 https://en.wikipedia.org/wiki/Gossip_protocol

广告投放矿工



在分布式系统中，CAP定理指出系统不可能同时实现以下所有目的：

- 一致性
- 可用性
- 分区容错性

因此，广告投放矿工的设计旨在满足响应XCHNG市场客户端发出请求时的一致性和可用性。

共识模型

在处理分布式系统时，分布式共识是一个众所周知的主题。虽然分布式共识可以复杂地解释，但也可以简单地定义为***在一组参与者中就一个得出的值达成一致的过程***。如果没有一个值被提出来，则没有值被选中。如果一个对等点提出并选中了一个值，其他对等点都应能够获知被选中的值。在不可靠对等点的分布式网络中，共识尤其重要。使用复制状态机的常用共识模型例子包括Raft[11]或Paxos[12]等协议。不过，各区块链平台正在实施和测试更多的共识模型，其中包括工作量证明 (Proof of work)、权益证明 (Proof of Stake) 和拜占庭容错 (Byzantine Fault Tolerance) 的各个变种等。

工作量证明

工作量证明（PoW) 最初提供了一种经济的手段来阻止针对服务的拒绝服务 (DoS) 攻击。PoW在比特币挖掘算法中更为流行。比特币使用Hashcash[13] PoW算法，这要求可设置的计算工作量。比特币中的区块包含随机数（nonce，在32位字段中只能使用一次的任意数字，使得该区块的哈希将以一串的0开头），矿工（添加区块的节点）挖掘nonce的方式是，区块的哈希值必须小于某个已知目标值。计算该值所需的算力很昂贵。但是，一旦找到该值，就可以轻松验证。生成新区块所需的时间称为基本块频率。

11 https://raft.github.io/raft.pdf
12 https://lamport.azurewebsites.net/pubs/paxos-simple.pdf
13 http://www.hashcash.org/papers/hashcash.pdf

权益证明

目前存在集中权益证明 (PoS) 共识模型的变种。不过，这种模型可以简单地定义为一种共识协议，用于赋予持有系统权益的实体维护分布式账本历史的能力。权益持有人拥有流通货币总量中的一小部分，因而有资格创建分类账中的下一个区块。如果安全性开始下降，权益持有人可能会损失对网络的一小部分权益。通常，PoS实现由验证节点组成，系统向这些节点随机分配提出新块的权利。一旦一个验证节点被选中提出一个块，会发生多轮投票。其他验证节点在每轮投票中对特定块发送投票。投票结束后，所有验证节点就哪个块添加到区块链中达成一致。

拜占庭容错

拜占庭故障可描述为对不同观察者呈现出不同症状的任何故障。此外，拜占庭故障是因要求达成共识的系统内发生拜占庭故障而导致的系统或服务失效。拜占庭容错 (BFT) 指系统防御拜占庭故障的能力。拜占庭泛指"拜占庭将军问题 (Byzantine Generals Problem)"。[14] 实用拜占庭容错算法 (Practical Byzantine Fault Tolerance，PBFT) 是一个能够容忍拜占庭故障的有趣的解决方案。[15]PBFT对每个协议采用三个阶段：准备前阶段、准备阶段和确认阶段。准备前和准备阶段用于完全排列发送给网络中对等点的请求。此外，准备和确认阶段用于确保确认的请求在所有视图中完全排序。

XCHNG共识

XCHNG为模块化共识机制而开发。运行不同的共识模型，例如PBFT、Raft、Paxos、PoS、PoW或混合解决方案很简单。我们的第一种方法是能够用PoS进一步增强的BFT解决方案。与其他PoS模型类似，我们的共识模型由一组验证节点组成。验证节点拥有的投票权数量基于网络中的状态数量。就一个交易或一组交易达成共识的一轮轮投票类似于上述模型。验证节点可提出、验证、准备和确认新的交易。当达成共识时，验证节点使用我们的P2P网络协议向其他对等节点广播交易。评级服务商监督验证节点。如果一个验证节点降至某一评级之下，将从网络中删除。在网络中有权益的任何人都可以成为验证节点。但是，鉴于通信费用，会对验证者的数量进行限制。

矿工参与新区块的创建。一个PoS共识模型被用于确定一个矿工对将生成的下一个区块的投票权数量。矿工在XCHNG网络中持有的权益越多，拥有的投票权也越多。矿工的权益起到了抵押品的作用，提高了矿工的忠诚度。

PoS减少了浪费的能源支出，而这种能源支出在PoW共识模型中却是必需的。此外，也不需要高端或定制硬件与其他矿工竞争。这些降低了简单参与网络的进入障碍。

---

14 http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.126.9525&rep=rep1&type=pdf

15 http://pmg.csail.mit.edu/papers/osdi99.pdf

跨链通信
随着区块链生态系统的不断发展，越来越多的实现涌现出来，成为区块链系统面临独特挑战的可行解决方案。为了适应技术的进步，XCHNG被设计为可以进行跨链通信。因此，XCHNG能与其他区块链实现进行通信。此外，XCHNG还能与当前市场上的其他去中心化应用程序进行交互。

第一方用户数据
XCHNG致力于提高媒体库存的价值，包括受众的元数据。除了传统数据管理平台外，用户还可将数据引入XCHNG市场。

用户数据存储在用户设备上。媒体和广告主不能直接查看用户数据。但是，当用户向XCHNG发布数据时，可以将其添加到媒体的库存中。广告主可以使用前文列出的相同市场协议定位用户数据。

XCHNG上的交易参与者举例
以下是XCHNG系统上智能合约IO的主要参与者。任何交易必需要有的参与者是买家和卖家。核心命名集内的其他参与者能提高市场效率和负责任度。

智能合约会对广告主（买家）与媒体（卖家）之间的交易进行编码，包括所有已被指定纳入交易的条款和行为。

买家
买家签订合约购买媒介。在数字广告业，买家也可以成为卖家，但对于一份合约，只有一个买家。

卖家
卖家签订合约出售媒介。在数字广告业，卖家也可以成为买家，但对于一份合约，只有一个卖家。

条款（非行为者）
条款虽不是行为者，但却是编码指令，构成了买家和卖家之间协议的条款。条款包括投放排期 (pacing)、目标定位、最低条件、价格和定价方法等。

测量服务商
鉴于条款的上下文，测量服务商能验证买家和卖家之间的合约。在数字广告业中，测量服务商必须支持协议中以编程方式概述的条款（例如投放排期、时段设置或广告展示次数的频次上限等）。例如，Kochava Inc.具有独有的地位优势，可成为XCHNG系统上的领先测量服务商，但因XCHNG是开放的，所以没有任何障碍阻止其他人成为XCHNG上的测量服务商。市场动态会推出这个方面或其他方面的最佳供应商。

测量服务商在XCHNG智能合约中是可选项。如果指定，具体智能合约的指定测量服务商将纳入合约及条款。

评级服务商
评级服务商基于所有历史交易对所有参与者提供评级，因此对XCHNG生态系统的健康至关重要。当XCHNG系统的区块链为每日滚动链时，这尤其有价值。评级服务商可提供库存评级、广告主评级、测量服务商或支付服务商评级或市场推动的任何其他指数。

评级服务商在XCHNG智能合约中是可选的。如果指定，具体智能合约的指定评级服务商将预先确定并纳入合约及上述条款。我们认为，被动评级服务商将进入市场，但它们将被降级为链上的公开数据，而非不在链上公布的重要信息。

XCHNG区块链有基本评级，由矿工完成，以确立网络节点的公开等级。尽管存在这种免费（且基本）的评级框架，但我们认为，商业评级服务商仍可为每个IO提供更详细的评级。

支付服务商
支付服务商能够为已约定并执行的智能合约提供支付支持，因而至关重要。支付服务商将遵守智能合约中规定的付款条款，并基于买卖双方条款中列出的重大支付节点以及测量服务商的确认进行放款。尽管支付服务商在XCHNG智能合约中是可选项，但我们认为XCHNG系统将为支付服务商应对数字广告中计费和收款方面的复杂性带来更大的价值。最后，如果指定了第三方托管服务（由支付服务商提供），则必须有参与的测量服务商，如果没有测量服务商在智能合约中发挥作用，将无法根据合约放款。与其他可选项一样，如果指定，具体智能合约的指定支付服务商将预先确定并纳入合约及上述条款。有一类公司很可能会发现作为支付服务商的价值，即基于要素的支付服务商，它们将能在收费的基础上向媒体提供加速支付。为了清楚起见，Kochava Inc.不作为支付服务商参与系统。

仲裁人

可选的仲裁人项目与测量服务商和支付服务商一起指定。如果买卖双方之间发生争议（仅在已指定测量服务商的情况下），由指定仲裁人处理争议。在选择智能合约的指定仲裁人时，将约定具有法律约束力的指定仲裁人相关条款。

XCHNG架构

XCHNG系统的独特之处在于，其架构被具体描述为能够支持指定参与者以及最初未想到的其他潜在参与者。此外，Kochava团队已将该技术平台构建为一个开放系统。XCHNG架构的核心是用于买卖双方交易的李嘉图智能合约。

智能合约

智能合约是定义了资产的交易指令、在区块链上执行的软件。智能合约处理参与XCHNG网络的成员商定的业务逻辑。账本状态仅限于具体的智能合约，其他智能合约无法自由访问。但是，访问权限可授予另一个智能合约，以访问交易状态。XCHNG API实施了一系列为使智能合约被视为有效而必须实施的标准接口。

智能合约生命周期

XCHNG API允许用户签署、部署、初始化和升级网络上的智能合约。目前还在开发其他功能，以使智能合约生命周期更稳健并且更易被最终用户管理。智能合约由所有者签署。针对经签署智能合约的所有操作都必须经过验证。智能合约一旦签署，就可以通过XCHNG API部署到网络中。部署完成后，智能合约的所有者可通过API向XCHNG网络发送其他命令，例如初始化或升级等。智能合约在初始化之后，就可以开始处理交易。

签署智能合约

智能合约在签署之前，必须满足XCHNG API中定义的初始接口。这个接口建立了一整套智能合约必须遵守的通用要求。智能合约必须在全部所有者先验证并同意其执行后，才能部署到XCHNG网络上。经同意后，所有者使用自己的密钥签署智能合约。签署智能合约即提供了所有权和验证。只有签署了智能合约的所有者才能执行部署、初始化和升级命令。

部署智能合约

智能合约签署后，即可部署到执行智能合约的XCHNG网络上。智能合约由一名所有者通过XCHNG API进行部署。成功部署后会创建一个地址。该地址用于向智能合约发送其他命令和交易请求。智能合约一旦部署，即可由一名所有者进行初始化。只有签署了该智能合约的所有者才能调用部署命令。

初始化智能合约

智能合约部署到XCHNG网络后，所有者可以对部署生成的智能合约地址调用初始化命令。成功初始化后，智能合约可以开始接收交易请求。只有智能合约的所有者才能调用初始化命令。

升级智能合约

智能合约的所有者可随时调用升级命令。若要升级现有的智能合约，所有者必须重新签署并部署新的智能合约。智能合约部署到XCHNG网络后，所有者可通过提供现有智能合约的地址来调用升级命令。这会将新智能合约指向原地址，以便交易能在新合约版本中进行处理。升级时，由终端用户管理智能合约的状态。只有智能合约的所有者才能调用升级命令。

理解XCHNG架构

虽然该框架将是开放式的，但一些生态系统合作伙伴（包括Kochava Inc.）计划发布工具以快速跟踪卖家和买家采用XCHNG系统的情况。XCHNG架构将在下文作进一步描述，该架构包括市场、市场协议、市场生命周期和XCHNG市场。

市场

市场是加速货物或服务交换的一系列协议。市场协议使买家和卖家能够直接进行交易。其他网络参与者或行为者可进行验证、评级、审计操作或以其他操作方式支持买卖双方的交易。市场协议是去中心化的。没有一家实体运营或管理市场。交易中，指定参与者之间的交易是透明的。透明度可基于市场协议的动态性，在交易的谈判阶段作出选择。

市场包括以下要素：库存信息、购买信息、信息匹配和交易完结。

1. **库存信息**
   库存信息是对卖家库存的陈述。卖家通过Put协议向市场提交库存信息。
2. **购买信息**
   购买信息是对买家需求的陈述。买家通过Put协议向市场提交购买信息。
3. **信息匹配**

买家和卖家将信息提交给市场。每个信息都添入市场信息列表。当两个信息匹配（即库存信息和购买信息的条款一致）时，买家和卖家达成一个订单。订单是买家和卖家的交易承诺，通过Put协议添加到市场的订单簿中。客户端将订单的交易发送到市场账本中。

4. **交易完结**
   客户端（买家或卖家）通过Put和Get请求与订单交互。XCHNG网络验证订单是否已正确执行。卖家生成密码证明，并由其他网络参与者（即买家或审计者）进行验证。证明经过验证后，网络将处理付款并从市场订单簿中删除订单。

市场协议

本节将对市场协议作高度概述。

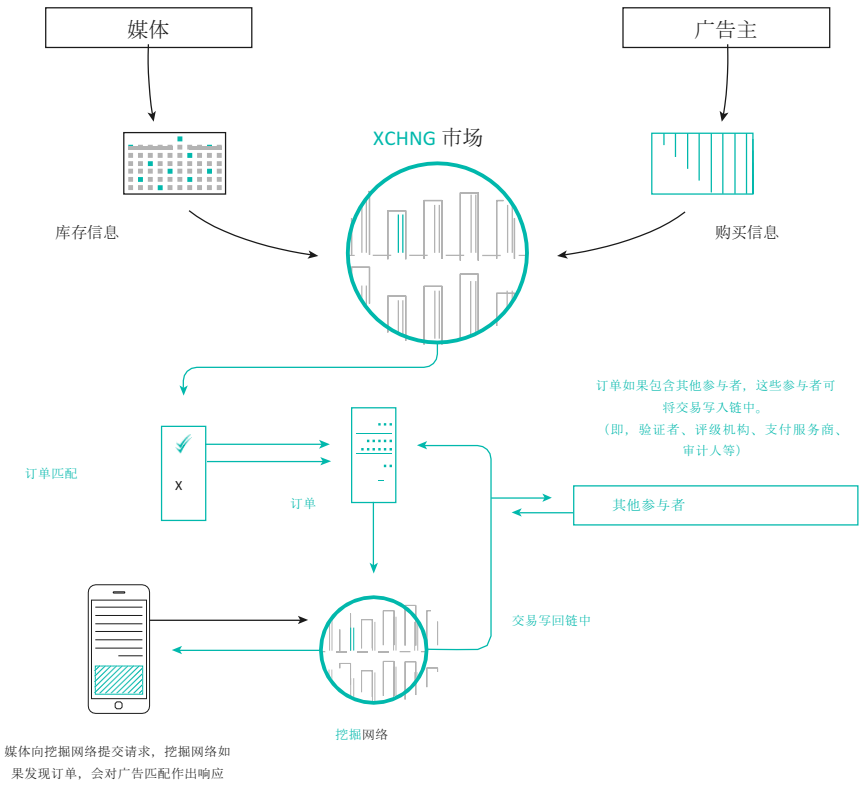
1. Put（发布）
   客户端（买家和卖家）可通过Put协议提交信息。各种Put协议包括：
   - Put.InventoryOffer：卖家通过Put.InventoryOffer提交库存信息。库存信息详述卖家想出售的东西，可包括价格、描述、数量等。
   - Put.BuyOffer：买家通过Put.BuyOffer提交购买信息。买家信息详述买家想购买的东西，可包括价格、搜索标准等。
2. Get（获取）
   客户端（买家和卖家）可通过Get协议访问自己的信息。各种Get协议包括：
   - Get.InventoryOffers:卖家通过Get.InventoryOffers访问库存信息。回应是卖家向市场提交的信息清单。如果匹配，每份信息可包含订单详情。
   - Get.BuyOffers：买家通过Get.BuyOffers访问购买信息。回应是买家向市场提交的信息清单。如果匹配，每份信息可包含订单详情。
   - Get.Order：买家或卖家通过Get.Order访问订单。订单可以公开，也可以私密，取决于买家或卖家的意愿。如果订单是私密的，仅订单中包含的参与者才能查看订单相关的交易。如果订单是公开的，则视为对全网络开放。
3. 匹配信息
   在客户端将信息提交给市场信息列表后，市场可以以编程方式或直接（即按买家和卖家）匹配信息
   - Put.MatchOffers：通过Put.MatchOffers协议匹配客户端引入的信息。客户端可以直接匹配信息。此外，市场还可以通过编程方式匹配库存信息，以购买其他信息。匹配的信息形成一个订单。

- Put.SubmitOrder：通过Put.MatchOffers创建的订单通过Put.SubmitOrder提交给市场订单簿。订单提交后，网络参与者可着手完成订单。

市场生命周期

市场生命周期概述如下。

XCHNG市场生命周期



1. **卖家客户端（媒体）**

   在任何新纪元时间（Unix纪元或Unix时间戳：从UTC时间1970年1月1日午夜开始流逝的秒数）可以：

   - 通过Put.InventoryOffer提交新的库存信息
   - 通过Put.MatchOffers查找匹配信息
   - 通过Put.SubmitOrder向区块链提交匹配的信息

2. **买家客户端（广告主）**

   在任何新纪元时间都可以：

- 通过Put.BuyOffer提交新的购买信息
- 通过Put.MatchOffers查找匹配信息
- 通过Put.SubmitOrder向区块链提交匹配的信息

3. **匹配信息**
   - 客户端通过相应的Put协议提交信息
   - 信息通过Put.MatchOffers进行匹配
   - 信息所有者共同达成订单
   - 订单通过Put.SubmitOrder提交给市场订单簿
4. **交易完结**
   客户履行订单后：
   - 双方确认商品/服务已交付
   - 卖家生成证据，其他参与者验证证据
   - 买家向卖家发送付款，确认有效且已交付的交易

XCHNG市场
XCHNG市场是一个促进数字广告购买、库存销售、跟踪、评级、支付和审计的市场实现。XCHNG市场实施前文所列的市场协议。

XCHNG客户端
媒体使用媒体客户端将库存信息引入市场。广告主使用广告主客户端将购买信息引入市场。信息通过XCHNG市场的Put.MatchOffers协议进行匹配。在匹配阶段，卖家（媒体）和买家（广告主）进行谈判。

在谈判阶段，执行共同的基于时间的拍卖协议，这让双方可以增量移动。例如，买家和卖家可以输入价格底线，该底线在信息匹配的谈判阶段将随着相关信息自动提高。

零知识证明
密码证明有一个常见的副产品，即除了使人确信陈述是真实的之外，还使其获知了一些知识。零知识证明试图避免双方之间的知识分享。双方包括证明者和验证者。此外，零知识证明可描述为一个交互式的概率证明，必须满足三个功能：完整、可靠和零知识。[16]

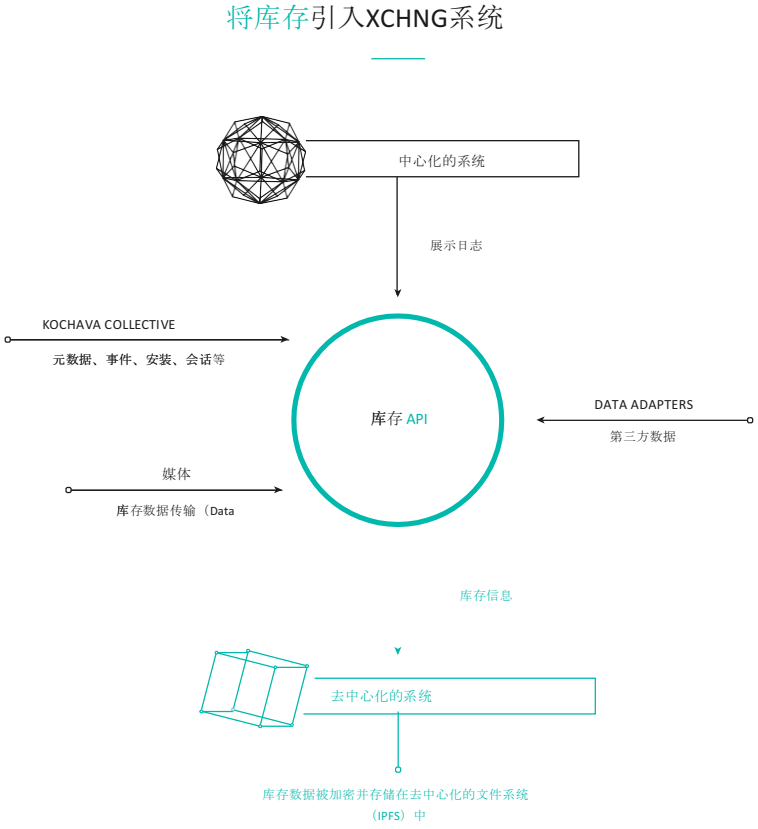
如果陈述是真实的，并且诚实的证明者使诚实的验证者（即遵循协议的验证者）确信这一事实，零知识证明视为是完整的。如果永远不能使用该证明得出虚假的陈述，则该证明是可靠的。如果陈述是真实的，并且除了知道陈述是真实的之外，没有任何恶意的验证者能够获知任何其他信息，则证明是零知识的。

16 http://www.cs.princeton.edu/courses/archive/spr10/cos433/lec17new.pdf

广告订单

在媒体和广告主之间完成库存匹配后，会提交订单。在XCHNG市场中，这些订单可包含定价、频率、分区、广告创意、持续时间等条款。经参与方批准，匹配的订单成为广告订单。这些智能合约IO可供参与者使用，满足订单条款的交易将被写回IO交易日志。

当媒体有可用于展示的库存时，向网络发出请求。XCHNG广告投放矿工响应请求，为展示查找适当的IO。



将库存引入XCHNG系统

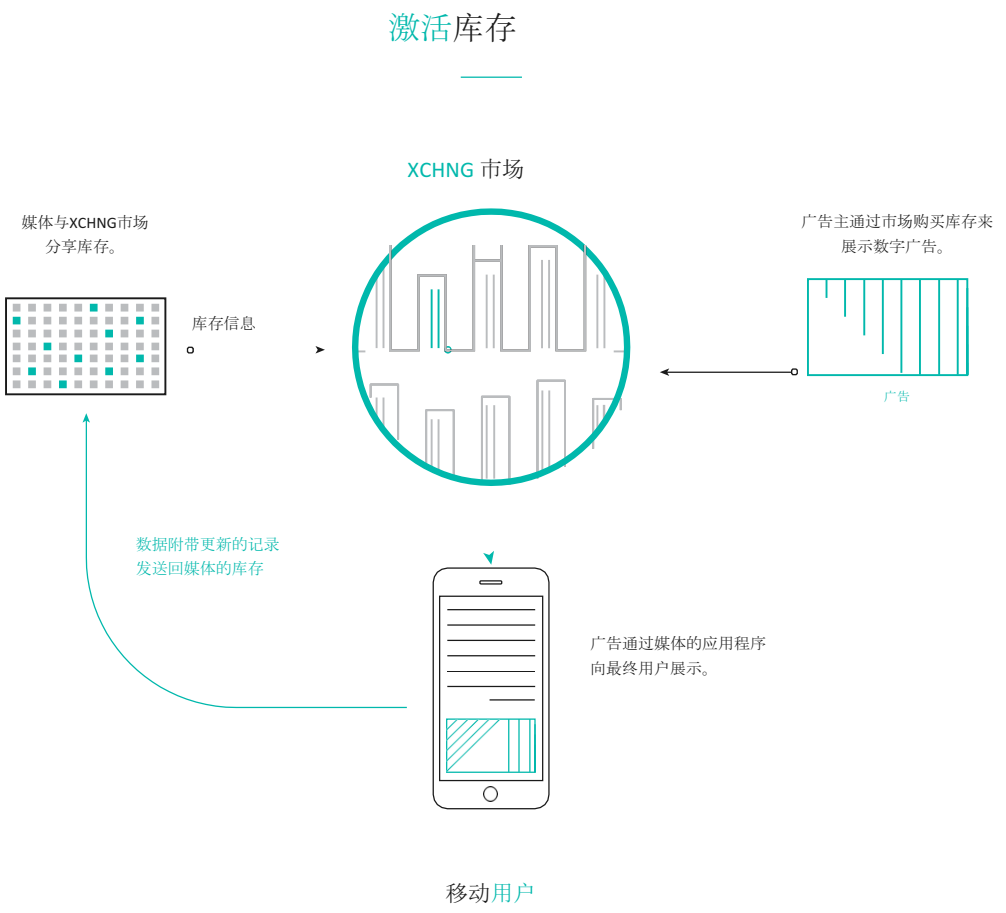
将库存引入XCHNG系统会在链上创建可寻址性链接。这表明特定设备可通过将该设备库存发布到链上的相关媒体源进行寻址。对于可在链上定位的设备，还可选择引入身份认证（经数字签名的认证，证明身份的真实性）。汇集多个库存源提供的设备属性，可验证设备的存在以及设备属性（如设备信息、在设备上运行的应用、使用行为、位置或其他元数据）的准确性。这种方法可以确保欺诈性库存不会在无不利后果的情况下被引入链条。

XCHNG的激励模型

为了激励库存源参与发布受众库存以及可用的展示量，XCHNG引入了激励模型，为供应源提供利益。

激活库存

XCHNG系统上的库存基于引入链上的库存和负责交付的智能合约IO，通过使用XCHNG在其开放式广告服务器和中介服务器上提供的工具启用广告展示进行激活。通过集成这些面向媒体的开放工具，XCHNG可以轻松采用，同时还可以利用现有广告动态。第三方广告服务器和中介服务器将能纳入XCHNG提供的代码，以在XCHNG上运行。



其他研发

网络分片

目前现有的区块链共识模型（PoW、PoS和BFT）通常落在可扩展性谱的不同侧。虽然PoW可以很好地扩展，可有大量的节点，但存在高延迟问题。拜占庭容错模型提供了高交易吞吐量，但会随着节点数量降级。随着越来越多的对等节点加入，网络带宽会开始限制交易吞吐量。通常，公共的非许可区块链中的每个对等点都需要处理每笔交易。网络分片的主要原则是将网络划分为更小的对等点组。这将减少每组负责的交易次数。

侧链

相关研究证明了网络分片能够如何提高交易吞吐量，而XCHNG还包含侧链。侧链指两个或更多区块链之间的母子关系。母链或根链中的智能合约含有对子链的引用。这使子集对等点能够处理与各自侧链有关的交易，减少自身负责的交易总数。每条侧链都使用密码证明链接回母链。每日滚动链 (DRC) 的想法有助于减少负责维护侧链的对等点所需的总磁盘空间。DRC将存储在侧链内的交易概述为密码证明，并将其写回侧链的母链中。XCHNG侧链模式与楔入式侧链 (Pegged Side Chain) 的概念思想一致。[17]

数字广告业最近的代币项目

尽管XCHNG项目引人注目，使用区块链技术整合了支持数字广告的整个圈子，但区块链领域还有一些其他项目，他们也在阐明其在广告业中的价值。我们想强调在我们看来他们适合的方面，以及我们的方法如何不同。

特别是，XCHNG不同于其他项目，因为该系统：

- 使数字广告中的所有参与者都能以各自目前的参与方式参与进来（避免颠覆性部署，而是鼓励演进性部署）
- 为现有参与者进行规模运营创造了新途径
- 为新参与者进行规模运营创造了新途径——推动更多的竞争
- 为广告主使用区块链实现（例如Kochava）上运行的商业工具进行大规模购买提供了一条清晰的路径
- 为媒体利用现有的货币化策略，以及随着使用XCHNG进行货币化得到证实而慢慢转向XCHNG提供了清晰的路径

17 https://blockstream.com/sidechains.pdf

adChain
虽然adChain提到将来广告业可通过区块链支持并帮助归因或端到端交易支持，但根据其白皮书，adChain主要是为了解决广告主向媒体提供欺诈报告的问题。adChain和XCHNG并不相互排斥，未来adChain计划可能会在XCHNG发挥作用。

AdLedger
AdLedger没有具体代币支持，支持它的是一些志同道合的专注于区块链技术标准化的管理者。Kochava有兴趣与AdLedger合作，并提出XCHNG系统是现实世界支持他们目标的具体体现形式。

Basic Attention Token (BAT)
Basic Attention Token主要关注在最终用户和媒体之间建立关系，从而保护消费者的身份并使消费者能够参与广告的价值链。BAT和XCHNG并不相互排斥，未来BAT计划可能会在XCHNG发挥作用。

结论

总之，数字广告生态系统进行革命的时机已经成熟。区块链是一种颠覆性技术，可以解决数字广告业目前面临的一些最大挑战：效率低、欺诈、缺乏透明度和缺乏标准化。区块链具有点对点、去中心化的性质，提供了一种新的范式，可使竞争环境更为平等并使所有参与者受益。Kochava具有独有的地位优势，可以将区块链解决方案引入数字广告生态系统。

OnXCHNG的合作伙伴

XCHNG的成功将与数字广告生态系统的采用直接相关，而后者依赖的框架需满足参与者的要求，并真正提供更安全、透明和高效的系统。Kochava Labs已寻找关键合作伙伴加入该项目。每个合作伙伴都将贡献自己的专业知识，提供指导并增加项目的曝光度。Kochava Inc.是最初的测量服务商，截止2017年底加入OnXCHNG的各类合作伙伴如下：AerServ、AppLift、Appodeal、Chartboost、Datawallet、DataStream、DCMN、Feedmob、InMobi、Instal、Kiip、Parrable、Payability、PubNative、Snap Interactive、Sulvo和YouAppi。每个合作伙伴的信息都将包含在2018年更新的白皮书草案中。

关于Kochava Inc.
Kochava Inc. (www.kochava.com) 为计划、定位、测量和优化广告支出提供了一个独特、全面、公正的分析平台。其移动和连接设备平台将强大的功能与全球数以千计的网络和媒体整合平台结合在一起，使广告主可以精准定位受众并测量广告活动的效果。实时可定制的可视化使用户可以流动访问全部数据点，这就向用户提供了强大的细分能力和实时可操作性。Kochava Inc.在该生态系统中提供了最强大的工具，因而被行业垂直领域中的品牌选择作为最大、最复杂广告活动的测量服务商。

Kochava Inc.具有理想的优势，将成为XCHNG上的第一个被引用的测量服务商。

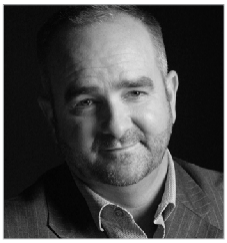
Kochava Inc.具有独有的地位优势，将成为XCHNG框架上值得信赖的测量服务商
Kochava Inc.集成了包括Facebook、Google、Snap、Twitter和Oath在内的几乎所有现有移动媒体资源以及AdColony、AppLovin、Vungle和InMobi等领先独立供应商。总之，有3,000多个与Kochava平台完成技术集成的广告网络和媒体资源。此外，Kochava Media Guide（媒体指南）拥有50,000多家拥有广告库存的注册媒体。今天，Kochava Inc.是一个记录系统，基于广告主的配置为其广告活动提供归因，每年测量的广告支出超过60亿美元。

请注意本白皮书第9页的LUMAscape数字广告生态系统公司图。Kochava Inc.已与该图上的所有部门合作。这些长期行业关系的范围和影响力非常重要。

目前，Kochava Inc.是测量服务商，没有经由XCHNG区块链的相关架构和框架。Kochava Inc.具有独有的地位优势，能够“聚合”非常庞大且复杂的行业围绕区块链开始广告标准化。

Kochava Labs SEZC是Kochava Inc.的研发子公司、XCHNG的架构师，Kochava Inc.将是颠覆性的第一个参考实现。这不仅仅是完全寄希望与行业能够采用的一个区块链工程师概念化项目用，Kochava Inc.和其他OnXCHNG合作伙伴都希望利用自身在生态系统中的权威和经验推动向XCHNG区块链的全面转换。此外，由于Kochava Inc.并非媒介提供商，因此当供应合作伙伴尝试“自评”时，Kochava Inc.不存在内在利益冲突。实际上，人们会戴着利益冲突的眼镜怀疑地看待广告业中源于媒体或其广告库存的任何区块链计划。这就是为什么独立于媒介和独立于风险资本证明了XCHNG系统背后动机的原因了。

XCHNG团队成员



Charles Manning
首席执行官，Kochava Inc.
董事，Kochava Labs SEZC
Charles Manning是Kochava Inc.的创始人兼首席执行官，该公司是领先的移动归因与分析平台，为全球一级广告主提供服务。近20年来，Charles一直在创造使用数据进行系统优化的技术，从商业服务管理 (business service management, BSM) 到信息技术 (IT) 再到归因分析，以及最近的区块链等等。Charles的职业生涯从Oracle开始，之后在M-Code、Managed Objects和PLAYXPERT担任过经理和总监职位。

在创建Kochava之前，Charles创立了PLAYXPERT，该公司最初是一个游戏技术平台。在将PLAYXPERT技术授权给Razer后，Charles建立了一个团队，专注于为企业家和代理机构构建参与平台。在认识到需要一个能进行有效归因或移动设备安装后分析的标准平台后，Charles及其团队创建了一个平台，Kochava由此诞生。目前，Kochava技术已与3500多个网络和媒体集成在一起，获得了数百个品牌的信赖，其中包括手机游戏、新闻和媒体以及消费品领域的知名品牌。

Breaux Walker
区块链高级副总裁，XCHNG
Breaux Walker是国际区块链和代币化业务拓展方面的领导者。作为Kochava的区块链高级副总裁，Breaux负责Kochava资助的开源区块链项目——XCHNG的业务开发。此前，Breaux曾担任中国上市金融科技公司——联动优势的国际高级副总裁。在此之前，他是宽资本的合伙人，投资过中国的金融科技、移动和互联网公司。

Breaux拥有10多年的投行经验，曾担任JMP证券投资银行集团的董事总经理，负责监督中国投资银行团队并管理公司与招商证券的合资企业。在整个职业生涯中，Breaux一直是中美移动和互联网领域的企业家和银行家，完成的交易超过10亿美元。中文说写流利。

Ethan Lewis
区块链架构师，XCHNG
Ethan是XCHNG框架的主要架构师。拥有莱特州立大学的计算机科学硕士学位，曾担任IBM公司B2B云服务部门的首席构建/自动化工程师，负责编写软件和培训新团队成员。Ethan曾在VR和AR领域工作，为无人驾驶飞机系统开发Sense和Avoid项目，并为内部应用设计和开发概念验证和集成测试系统，始终注重优化速度和功效。Ethan熟练掌握Golang、Java、Python、C ++和其他许多语言和技术，对区块链和分布式账本技术有特别的热情和经验。

David Matt
总经理，Kochava Labs SEZC
David是Kochava Labs SEZC的内部顾问并负责开曼群岛办事处。拥有贡萨加大学法学院法学博士学位。David的专业领域包括公司法、并购、知识产权和数据隐私。此前，David曾在DMS Worldwide担任过7年的业务顾问。此外，还有14年经营各种企业的经验，主要在服装生产领域。

Doug Lieuallen
董事，Kochava Labs SEZC
Doug Lieuallen有25年的财务主管经历，从初创企业到公共实体不等，涉及技术、广告和零售等行业。作为Kochava的首席财务官，Doug在公司的整体管理中发挥了战略性作用。主要职责包括会计、财务规划和分析、资金、并购、法律和行政等职能。
Doug担任过多个财务和会计领导职位，在Kochava任职之前是业务规模达7亿美元的零售商Coldwater Creek的资金运营高级总监，此前曾担任Wieden + Kennedy 伦敦公司的财务总监。在其职业生涯中，Doug一直负责创建可扩展的全球运营并为此提供资金。

作为Kochava Labs的董事，他负责监督Kochava资助的开源区块链项目XCHNG并为此提供专业知识。

Kimberly Manning
品牌总监，XCHNG
Kimberly拥有丰富的营销经验，专注于品牌创建与管理。她是Kochava Inc.的品牌总监，曾自创设计公司并担任负责人达12年，为高科技、生物技术、消费品领域的客户及非营利性组织客户提供品牌塑造、营销和内容创作等服务。Kimberly对区块链以及如何使分布式账本技术触达更广泛的受众并能被更广泛的受众理解有特别的热情。

Matt Hrushka
产品经理，XCHNG
2015年以来，Matt一直投身于加密货币领域，对包括区块链在内的分布式账本技术有深入的了解。此外，Matt在数字广告领域具备专业经验，因此有能力理解使用区块链来解决该行业的挑战。Matt曾担任Rosetta Stone的移动营销经理，此前是Verve Mobile的广告运营经理。Matt是OnXCHNG合作伙伴计划的主要联系人，对于为XCHNG项目引入新合作伙伴充满热情。

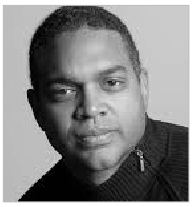
人才团队
Kochava Labs SEZC已就XCHNG的开发和营销与Kochava Inc.签约。除上述个人团队成员外， Kochava Inc.的150名员工还会为项目提供的全面的专业知识，包括管理、开发、营销和客户服务各个方面。

XCHNG顾问

Kochava很荣幸地欢迎XCHNG项目的诸位顾问，他们是数字广告、区块链技术和加密货币等各方面经验丰富的专家。他们的参与将继续引导XCHNG和XCHNG代币的发展。

Mark Beck
Murka战略副总裁

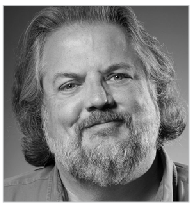
Paul Cheng
Ericsson Emodo总经理
在互联网、移动、广告科技、营销科技和加密货币/支付行业具有丰富的管理和顾问经验。



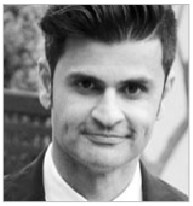
Terrence Coles
AddApptr有限公司总经理、Smaato前总经理

Mark Connon
美国在线平台和广告公司 (AOL Platforms & Advertising) 前高级副总裁兼全球首席移动与数据官

Jeff Coon
InMobi前全球联盟副总裁，曾任Quantcast的业务拓展总监

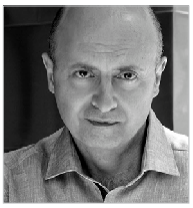


Ernie Cormier
曾任Nexage首席执行官，专注于运营损益责任、战略、产品、技术/工程、营销与品牌、销售、商业与企业发展



Paran Johar
现代营销峰会 (Modern Marketing Summit) 全球首席执行官

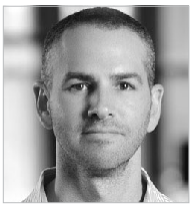
John Maffei
Matcherino首席执行官
Servicemesh前首席执行官、ZAM网络前总裁



William Mougayar
战略、营销和增长方面的顾问、投资人、导师、科技企业家和创始人。国际讲演人、《商业区块链：下一代互联网技术的承诺、实践和应用》的作者。

Stephane Panyasiri
Kochava Inc.欧洲、中东和非洲区总经理、SEA Gaming Pte Ltd前首席执行官

Krish Sailam
Cadreon西海岸方案策略副总裁



Jeremy Sigel
Essence合作伙伴关系与新兴媒体高级副总裁

Andy Sippel
Advertiser Perceptions高级副总裁、今日美国体育传媒集团前高级副总裁

David Wachsman
全球最大区块链公关机构Wachsman创始人兼首席执行官

Bob Walczak
WPP程序化广告购买平台Xaxis的前全球产品执行副总裁

Kevin Weatherman
OneSignal的业务拓展副总裁、MoPub的前业务拓展/销售副总裁、Twitter前全球媒体销售总监

David Weild, IV
前纳斯达克副主席
Weild & Co. Inc.创始人、董事长兼首席执行官，该公司是投资银行公司Weild Capital, LLC的母公司。Weild也被称为JOBS法案之父，曾参与起草美国国会立法。