The AdChain Registry

2017 年 5 月 31 日

Mike Goldin
ConsenSys

Ameen Soleimani
ConsenSys

James Young
MetaX

翻译&校对：EthFans 以太坊爱好者

简介

在数字广告市场中，广告主每年因为机器人无效流量而被骗支付的费用高达 180 亿美元。[1] 不透明的供应链为机器人运营商打掩护，使得这些运营商可以隐藏在广告交易所的黑匣子背后，并隐藏在不被监管的广告生态后。[2] 由于广告主下游的供应链实体通常以每千次展示成本付费（CPM, Cost Per Mille）的方式付费，所以这个经济激励导致他们只为了最大化广告曝光次数，而无需在意这些曝光次数到底是来自于人眼还是机器人。由于使用机器人极其廉价且难以被察觉，所以从经济最大化的角度来看，产业下游商户故意向机器人提供广告也是合情合理的。

由于自己的钱财就这样被窃取，广告商也随之变得十分心灰意冷。[3] 程序化广告购买相对于直接广告交易，无疑是量化广告购买商价值最大化的必经之路。同时，程序化广告购买也是数字广告业务增长最快的领域。但就目前来说，程序化广告交易在推广不可安装的商品时广告效率相对较低。[4] 人们在网页上的行为很容易为机器人所模仿，而在网络上发现那些自动机器人的行踪从本质上来讲就是一个猫鼠游戏。[5] 这使得广告主大多数情况下面对这种向下供应链的激励体系无能为力。

AdChain Registry 是一个由 ConsenSys，MetaX 和数据和营销协会（DMA）联合推出的去中心化持有的域名白名单。DMA 是一个拥有 1,400 名活跃成员和超过 100,000 名参与者的行业组织。 AdToken 的持有人通过一个激励性投票的方式来确定希望加入注册表的申请人是不是一个合法且可信的广告发行商。代币持有者们不会因为广告发行商的曝光量增加而获益；相反，代币持有者们在注册表中申请加入或更新注册状态的广告发行商的数量上升时才会受益。只要注册表能保持干净，即不含有机器人造成的无效流量，那么广告主就会希望向这些注册表中的广告发行商出价。同时，只要广告主愿意向这些注册表中的广告发行商出价，那么注册表中的广告发行商就会希望能保留在表中，且没进入注册表的发行商们就会希望申请加入。代币持有者们因此有动力来将欺诈的申请人从注册表中移出，并通过谨慎地投票来维持这种良性循环。

The adChain Registry

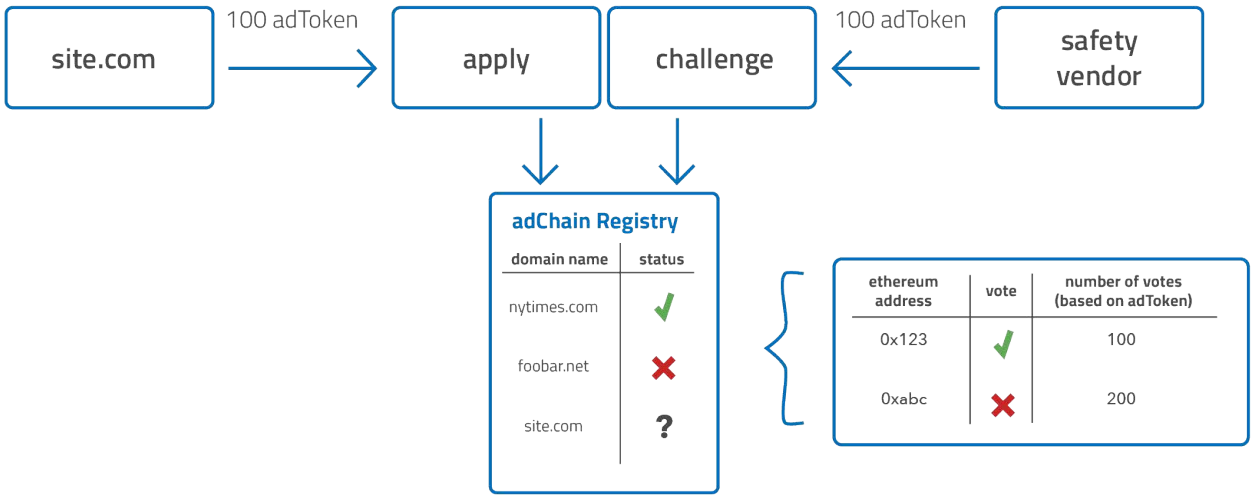
AdChain Registry 是一个基于以太坊区块链技术的智能合约，该合约存储了由 AdToken 持有人鉴定为“非欺诈性”的域名列表。 注册表中会出现 foo.net 域名，意味着 AdToken 的持有人在近期审核了该域名，并认为它归属一个拥有真正人类受众的合法广告发行商。

这个注册表也由多个交互组成。其中一个是代币持有者推荐新域名加入注册表的交互，另一个是对这些推荐提出反对的交互。还有一个是当出现反对时代币持有者在对结果进行投票的交互。

---

1 “Ad Fraud Estimates Double”. WPP. Business Insider. March 16, 2017.
2 “The Methbot Operation”. WhiteOps. Page 10. December 20, 2016.
3 “Chase Had Ads on 400,000 Sites. Then on Just 5,000. Same Results.”. Sapna Maheshwari. The New York Times. March 29. 2017.
4 “Interview with MachineZone CEO Gabe Leydon”. Recode. February 24, 2016.
5 “Mystery Shopping Inside the Ad Fraud Verification Bubble”. Shailin Dhar. June 8, 2016.

最终，还有一个 AdToken 持有人可以通过投票更改注册表中常量参数的交互，例如正在申请中的广告发行商可被反对的期限。



登记申请及数据

如果广告发行商想申请被录入 AdChain 注册表，他们需要提交一个域名，例如 foo.net，和一份 AdToken 作为保证金。这份申请会被放入一个申请池，并带有有一个考察期，如果考察期期间无人提出异议，则通过考察，域名被登记到注册表上。

被录入 AdChain 注册表中仅在一个有限的时间期内有效。因为域名可以被出售的且域名质量可能会随着时间的推移而下降，因此一个在今天还算高品质的域名也许到了明天就不怎么样了。广告发行商可以在其认证失效之前申请更新注册，如果成功更新，就不会导致该域名认证状态的中断。当某一注册的认证失效时，当初打入智能合约的该域名 AdToken 保证金可以由原始申请人提现。

注册可以包含额外且可选的更多数据，例如注册人是否接受 BAT [6] 付款方式或者是否遵守 AdChoices 标准的认证。

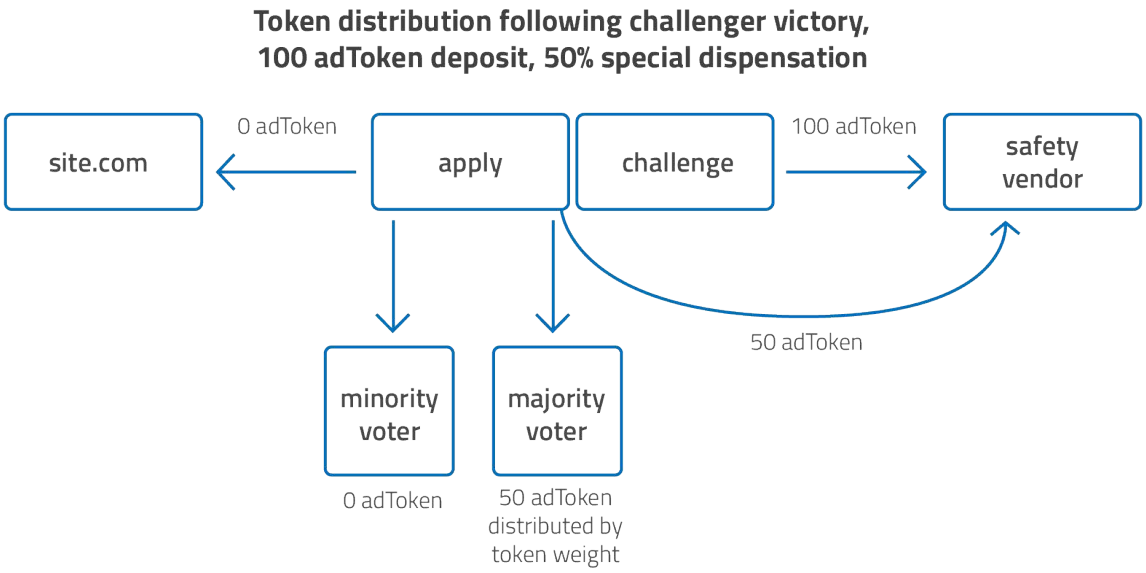
登记申请质疑

带有明显欺诈性质或低质量域名的申请将会受到理性 AdToken 持有者的质疑。要在考察期间针对登记申请提出质疑，代币持有人必须存入与申请人所存保证金数额相等的 AdToken。这样做会启动一个投票期，在此期间，代币持有者将会进行代币加权投票，决定申请是否被批准。投票方案是承诺 – 揭露式（commit-reveal）的，这种模式起源于 Colony 的部分锁定代币加权投票系统。

[6] "Basic Attention Token (BAT)". Brave Software. May 23, 2017.

如果考察的结果有利于申请人，那么质疑者的保证金将被没收，申请人的域名将被列入 AdChain 注册表中。如果考察有利于挑战者，申请人的保证金将被没收，且申请人的域名不会列入 AdChain 注册表中。如果申请人的申请失败，只要他们愿意，他们可以随时重新申请登记。

当投票结束时，被没收的保证金会按百分比直接奖励给在投票中获胜的一方（无论是申请者还是质疑者）作为一种特许分配。剩余的保证金按照参加投票代币权重在获胜集团的投票者之间按比例分配。而失败集团中的投票者则什么都得不到。



在考察中，获胜方的保证金永远会退回到他们手中。因投票而锁定的代币则总是归还给其所有者，无论他们是投票给胜利方还是失败方。只有在考察中失败那一方的保证金才会被重新分配，且不能由其原始所有者追回。

注册表的参数化

AdChain 注册表中没有恒定参数（“magic number”）。注册表将根据创建者的最佳估计，以合理的初始值开始运行，但所有这些参数都可以通过 AdToken 持有者的投票并重新设置。截至目前为止，提到可参数化的值包括：申请保证金金额、考察期长度、注册有效期限、代币投票的投票期以及审核期以及以代币形式分配给获胜方的比例等。整个治理系统本身的参数也可以根据投票改变，如启动改变参数所需的代币份额等。

可以以挑战获胜方特许奖金分配金额为例来思考注册表中常量值的参数化对博弈机制的影响。理性的参与者是否发起挑战的决定是基于对潜在收入的考量上的，此考量取决于挑战者的预期收入以及对挑战胜利概率的判断。挑战者如果没有通过代币投票则将失去全部的保证金，反之，如果通过代币投票，则可以赢取一定数量的原始保证金。如果特许分配金的比例设为 50%，那么理性的被考察者必须有超过 66%的把握来赢得代币投票并发起挑战质疑。

AdToken 的供应总量是不可由投票改变的，AdToken 既不能通过挖矿生成也不能被销毁。 10 亿个经实例化部署的 AdToken 会永久成为 AdToken 不可更改的固定数量。

广告主，发行商和 AdToken 持有人之间的良性激励架构

数字广告中的大部分付款方式都是基于 CPM 结算。 CPM 是一种极为反常且不正当的激励模式，是广告技术中多数罪恶的根源。简单来说，广告商会向发行商支付每千次展示所需的固定金额，即 CPM 。 但 CPM 模型的问题是，展示次数对于访客实际关注率来说是一项弱指标。一部分原因是因为展示次数是一种高度抽象的概念，不同供应商可能以不同的方式进行估算。广告主的下游供应商有动力来以十分宽松的方式来评估展示的来源。

在从广告主到发行商这一案例中，发行商并没有动机报告某次网页浏览到底是不是一次完整的浏览过程。实际上，由于机器人很容易在网页上模仿人类行为，因此广告发行商购买机器人浏览广告并将浏览结果报告给广告商便是经济而合理的。广告主希望仔细审查他们收到的浏览数据，但这一审查过程从本质上是不可计算的，只能利用统计学进行猜测。程序化购买供应链中存在大量中介机构使得这个问题更加严重。单次广告展示可以在位于广告主和发行商之间的数十方之间进行交易。由于任何报告欺诈行为的一方都会通过这种方式自行收取收益，所以发行商的激励架构与广告主下游所有各方的激励架构完全相同。

AdChain 注册表的关键创新点在于它通过将注册表所有者（AdToken 持有人）的奖励机制与 CPM 脱钩，从而鼓励有信誉的发行商。代币持有人只关心一个问题，即需要标记池中具有欺诈性和低质量的申请人，并赢得投票以拒绝这些申请。投票的焦点围绕着申请人是否具有欺诈性或是否资质过低。通常，理性的投票者会以集体的方式决定接受还是拒绝对于某一投票者在这两方面的评估。那些理性且尽职尽责的投票者着会获得奖励，而失败一方的不那么尽责的投票者则会招致机会成本的提高，因为表决期间锁定 AdToken 价值没有提高。

要想关闭广告商、发行商和代币持有者之间的良性激励循环，必须要理解最后一点。 对广告欺诈投票的行为中存在一个隐含的大前提，即投票结果会增加 AdToken 的价值。虽然这个概念应该与欺诈的概念紧密地联系在一起，但这一概念本身就是有价值的。

[7] There is a 33% chance of -100% deposit and a 66% chance of +50% deposit. (0.33)(-1) + (0.66)(.5) = 0.

考虑到质疑申请只能在申请人池中有申请人时才可发生。挑战游戏只能在申请人池中有申请人时才可继续， 申请人只会在发行商希望使用 AdChain 注册表刊登广告时才会申请进入 AdChain 注册表。只有广告商希望服务注册表中的发行商广告空间的报价请求时，发行商才会在 AdChain Registry 中提出或更新列表。发行商才会渴望在 AdChain 注册表中提出或更新列表。反过来，只有注册表环境相对于其他广告网络和白名单相对纯净时，广告主才会渴望向来自于 AdChain 注册表中的发行商提供广告位的报价。在这种情况下，代币持有人被鼓励通过对可疑申请人进行考察并投票排除带有明显欺诈行的申请来使注册表保持清洁。

从保证金和投票的角度来看，AdChain 注册表中的机制设计与区块链中的权益证明有很多共同点。关键的区别在于区块链验证块时，整个过程是可计算的，而 AdChain 将域名验证为非欺诈时，整个过程是不可计算的。因此，AdChain 探讨使用抵押协商机制在不可计算领域建立单一真相来源的一般模式。AdChain 并不旨在直接解决广告欺诈行为，而只是促使广告业界就欺诈行为及其界限的判定达成一致。

注册表的实际运用

AdChain 注册表提供了一个高质量、零成本的白名单，广告主可以通过阅读这一名单来决定是否为该广告机会出价。然而，AdChain 中的注册表的最小内容单位只不过是一个域名加一项认证状态指标。假设没有任何身份验证方案，如果 foo.net 是 AdChain 注册表中的认证注册人，那么机器人代理机构可以通过简单地更改其出价请求消息的原始标头信息来轻易地模拟 foo.net。

广告主需保护自己免受一些琐碎攻击。在这些攻击中，机器人代理机构可以通过欺骗原始标题 b 机器人来模仿 AdChain 注册人。虽然注册表本身对此不会做出反应，但对于整个行业而言，以统一的方式相互认证对各方都有益。使用传输层安全（TLS）的双向身份验证，即一种广泛使用的并且已经过实战测试的技术套件可以解决此问题。TLS 的单向握手协议支持网络上 HTTPS 连接的身份验证。双向 TLS 握手协议则支持广泛使用的 SSH（Secure Shell）协议中的身份认证。

本部分还讨论了一种由 MetaX 提供的，使代币持有者能轻松地与 AdChain 注册表进行交互的工具，并与 DMA 数据和营销协会（一个拥有 1,400 名活跃成员和超过 100,000 名参与者的行业组织）建立了合作伙伴关系。该组织愿意引导项目在现有行业状况下的进一步发展。

使用 TLS 的相互认证

通过将身份验证从应用层推出并进入广泛使用的传输层技术（如 TLS），AdChain 注册者可以在 RTB，VAST，VPAID 或任何其他标记格式（包括尚不存在的标记格式）下进行广告商务活动。这也意味着可以利用现有的生产就绪的软件来进行身份验证，并且新用户的注册成本仅仅是在 Web 服务器配置文件中写几行代码。

使用 Web HTTPS 方式中的证书签名密钥进行双向 TLS 身份验证足够对 AdChain 中的用户进行身份验证。在 foo.net 网络上用 header 标记来源并提供出价服务的广告商会要求发送者在 TLS 握手协议中进行相互验证。接受者则期望使用一个可验证密钥来执行身份验证，该密钥由受信任的证书颁发机构发布的 foo.net 的 SSL 证书进行验证。

广告商服务器执行以下分支逻辑关系：

1. 客户端可以通过 TLS 执行相互验证吗？
2. 如果可以，客户端在 TLS 握手中认证是否正确？
3. 如果正确，该域名在 AdChain Registry 的清单中吗？

如果以上任一问题的答案是“否”，则服务器分支执行任意逻辑关系来处理该情况。 支持 AdChain 成员的身份验证并不意味着广告商必须放弃与非 AdChain 成员的业务。

在供应方面，提供报价的实体必须能够使用注册者的证书签名密钥在 TLS 中进行身份验证。 技术精湛的发行商可能会选择运行自己的广告服务器来保留对其证书签名密钥的控制权。然而，大多数发行商都习惯于与提供招标和报价广告的供应商合作，且他们只要求供应商在其网页上嵌入 Javascript。 采用相互认证机制意味着供应商或者必须申请被列入 AdChain 注册表，或者必须与发行商控制的签名服务器交互。

理性代币投票者应该倾向于拒绝供应商之应用，因为聚集来自多个发行商的供应商很难加以审核，且这些供应商可以轻松地将机器人的无效流量隐藏于合法流量之中。签名服务器的方法就像一种快乐的中间地带：即使对于希望保留其证书签名密钥控制的相对不成熟的发布者而言，部署签名服务器也不会困难，并且该任务也可以委托给专门的服务提供商完成。

另一种方式，发行商只需将其证书签名密钥委托代理。 共享证书签名密钥需要对代理的高度信任，但复杂的供应商可能能够使用此模型建立业务。

投票交互

虽然 AdChain 注册表可以成为以太坊公有链上一个任何人都能平等使用的智能合约，但 MetaX 打算提供一个包含注册表的用户界面，以便代币持有者可以通过网络浏览器参与投票过程。代币持有人可以利用这一界面申请加入注册表，进入考察期，对考察进行投票并对注册表本身的参数化进行投票。 虽然这一界面是可选的，但它应该能使更多的访客可以访问。

由于公有链上智能合约的性质，任何人都可以选择自己编写自己的 GUI 包装器。通过像 MetaMask、MyEtherWallet、Mist 或命令行这样的工具与注册表进行交互显然也是有效的。

与数据和营销协会（Data & Marketing Association）的合作

> “看到智能初创企业为解决行业内欺诈、营销人员与客户的关系恶化等问题提供创新解决方案是十分令人振奋的。作为营销和广告行业中唯一代表行业生态系统内各方的行业协会，DMA 非常渴望看到其成员能像 MetaX 那样，提供创新的和以信任为基础的解决方案，为客户和供应方解决广告欺诈和其他系统内的痛点。”
> – Thomas Benton，数据和营销协会（DMA）首席执行官

数据与营销协会 （“DMA”）是一个行业协会，由超过 1,400 个电子广告生态系统中的需求和供应机构组成。 DMA 已经同意代表 adChain 在行业内进行推广，并将这个科技向业内教育和培训。DMA 对于利用 adChain 注册表技术来屏蔽欺诈行为保护自己协会的成员有着十分浓厚的兴趣。MetaX 将会负责向 DMA 提供区块链相关的技术培训和推广材料、demo 以及可以证明 adChain 价值的数据。DMA 也会成为 adChain 协会（ACA）的一名成员，ACA 协会是一个用来指导 adChain 协议发展和运用的非营利性组织。

项目管理

相对于其它代币化协议，AdChain 的一个独特之处在于它雄心勃勃，立志通过为业内成员提供管理工具，以及自上而下地推动该行业来解决现有行业面临的巨大难题。Brave、Gnosis、Golem、Melonport 和 SingularDTV 等公司正在创建区块链平台，与现有平台竞争，然而这些平台采用自下而上的发展方式，是一种必然有效的方式。由于支持现有广告技术产业存在挑战性，AdChain 的设计从一开始就受到了促动。该平台的复杂性并不完全体现在其协议本身，而体现在如何使该协议和现有行业参与者之间进行交互。因此该协议进行了刻意的简单化；如果系统过于复杂，那么行业参与者便难以确定自己在其中的位置以及最佳策略，将影响其采用策略的速度。

管理有可能成为该项目取得长期成功的关键因素。ConsenSys、MetaX 和 DMA 均意识到，具备区块链专业知识，数字广告以及在广告业的影响力对一个项目的成功来说缺一不可

参与组织

ConsenSys 是一家创业生产工作室，为以太坊区块链建立去中心化应用程序、系统、开发人员和终端用户工具。ConsenSys 于 2014 年在布鲁克林成立，是一家跨越六大洲，并拥有 200 名员工的全球性机构。ConsenSys 的企业咨询机构为世界十强企业设计并构建了基于以太坊的区块链基础架构。ConsenSys 是 BlockApps 和 Gnosis 公司的孵化器。ConsenSys 的广告技术实践被称为 CAT，将围绕 AdChain 构建应用程序和服务。

MetaX 是一家致力于为数字广告业开发并采用开放平台的区块链技术公司。该公司位于洛杉矶，能够以一种安全可靠的可扩展方式协调数字广告供应链。欲了解该公司的更新信息，请访问：http://metax.io

数据和营销协会（DMA） （www.thedma.org）：该协会成立于 1917 年，推动了一整个世纪的数据和营销议程，数据和营销协会通过对数据驱动式营销的创新和负责任的使用，提高了消费者参与度和业务价值。DMA 成员由 1400 多个品牌领导组织组成，包括如今的创新型技术和数据公司、营销商、代理商、服务供应商和传媒公司。DMA 代表整个营销生态系统——需求方和供应方——每年吸引超过 10 万名业内专业人士，具有独特地位，可以召集并引导行业将双赢方案引进市场，并确保可以迅速应用创新性和突破性营销技术，提高投资回报率。.

DMA 推动了数据驱动型营销行业的发展，并通过四个主要领导核心为其成员服务：倡导营销人员负责任地收集并提炼详细数据以识别并满足客户的需求和兴趣；通过创新方式解决数据和营销生态系统的最大挑战；教育当今数据和营销生态系统的成员要在渠道不断增多的世界中发展并领导营销组织；并联合行业参与者与时俱进，学习最佳实践，并通过&THEN （最大的全球性数据驱动型营销事件）和 DMA 一系列其他现场活动获得新兴解决方案。

The adChain Association (ACA)：是一个非营利组织，旨在协助采用、使用并管理 AdChain 协议。该非营利组织的详情仍需待定，一旦确认，将立即公开分享。ACA 的目标是通过指导 AdChain 协议更新和改进开放技术来推动数字广告行业的发展。ACA 认很重视去中心化，将促进这一目标的达成。

团队

Mike Goldin

Mike 于 2015 年夏季成为 ConsenSys 的实习生，开始致力于以太坊区块链的应用，从事 Ujo Music 智能合约后端的相关工作。他毕业于哥伦比亚大学，获得了计算机科学学士学位，之后便入职 ConsenSys，在 ConsenSys 企业集团担任软件开发员和架构师，目前是 ConsenSys AdTech 的技术主管。

Ameen Soleimani

自 2016 年夏季以来，Ameen 一直是 ConsenSys 的软件开发人员。除了 AdChain 以外，他的项目还包括点对点能源市场，去中心化对冲基金和状态通道研究。加入 ConsenSys 之前，Ameen 曾在伦斯勒理工学院学习化学工程，创立了波多马克代码营（Potomoc Code Camp），教授中学生基础编程知识，并创建了一个叫 Filter 的个性化新闻阅读器。他现在是 Moloch Ventures 的创始人，Moloch Ventures 是一个区块链企业生产工作室，专注于状态通道和代币化智能合约平台。

Mark D'Agostino

Mark 过去十年来一直在从事管理咨询方面的工作，尤其专注于金融服务行业。在加入 ConsenSys，成为该企业集团的管理合伙人之前，Mark 扩大了 Deloitte 的区块链市场供应。他已经成功向世界 500 强银行、全球性能源公司和政府交付了基于以太坊的应用程序。在其职业生涯中，他已经为 AIG、BlackRock、Citi、GE、JPM、Lehman Brothers、MasterCard 和 Pfizer 等客户提供过服务。在与 AdChain 的合作中，Mark 推动了战略和业务发展。

Miguel Morales

Miguel Morales 是一名经验丰富的全能工程师，专注于产品开发、架构和敏捷流程。他专门从事大型系统和数据管理平台的建设。Morales 在广告技术生态系统建设方面拥有深厚的垂直专业知识，特别是在移动和程序驱动型举措方面。他目前是 MetaX 的产品工程师，主要致力于 AdChain 计划和由 MetaX 开发的相关去中心化应用程序。他最近在 ZeroX 和 The Mobile Majority 工作。

James Young

James 拥有 20 多年的软件开发经验，专门从事流媒体视频网络设计和社交/手机游戏开发。他在 InterVU（第一个视频内容分发网络，之后又被阿卡迈公司收购）工作期间，第一次收购了创业公司。他也在像 Cisco 这样的大企业，以及像 Zynga 这样的知名创业公司工作过。在前互联网嬉皮士时代期间，他试过去 HotWire 找工作，自那以后一直对开放网络保有兴趣。

Ken G. Brook III

Ken 是一个企业家，从 2010 年起从头开始创立技术公司。他最近合作创立了 MetaX，并担任了首席执行官一职。MetaX 是第一个将区块链应用于数字广告的平台。最近，Ken 成立了 VidRoll，目前仍然担任首席执行官一职。VidRoll 是高端内容发布商的视频技术和货币化合作伙伴。此前，Ken 于 2013 年创建了跨平台的广告技术公司 StreamRoll Media，更早之前还在传统媒体和数字媒体领域任过职。

顾问

Raleigh Harbour

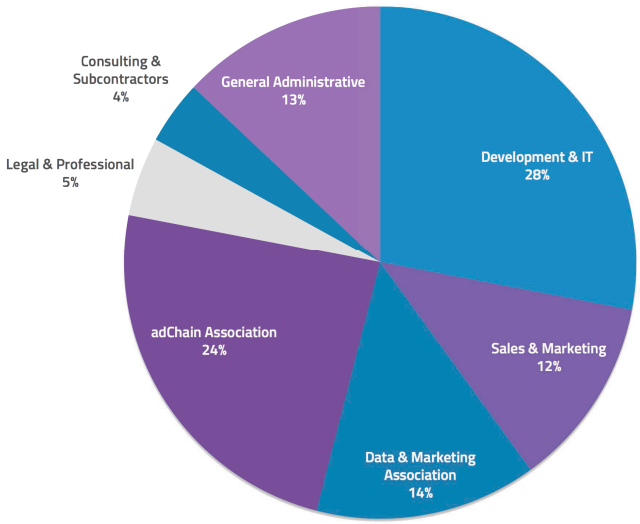
Raleigh 是一名经验丰富的执行官，在 SaaS 软件、在线媒体、数字广告和商业服务领域有近 20 年的经验。Raleigh 目前是 ATON Fortis 的执行合伙人。ATON Fortis 位于洛杉矶地区，是一家与技术创业公司合作的战略咨询公司。此前，Raleigh 曾任 AOL 的客户服务和营运高级副总裁，领导一个团队负责将 AOL 转变成一个可扩展平台公司。Raleigh 通过收购 Adap.tv 加入了 AOL，在其中担任首席运营官一职，负责该公司的全球运营。在收购 Adap.tv 之前，Raleigh 是 Rubicon Project 的商业和企业发展高级副总裁。Raleigh 拥有弗吉尼亚大学的文学士学位和芝加哥大学的工商管理硕士学位。

Shailin Dhar

作为少数真正独立的广告欺诈顾问之一，Shailin 撰写了《关于广告技术的非常识认识（Uncommon Sense for Ad Tech）》，一则关于广告的权威文章，史无前例地详细介绍了该主题。Shailin 作为一名程序化交易员，在多年工作中掌握了少有人了解却广泛应用的套利和流量采购实践的第一手经验，为广告技术行业提供了大量鲜为人知的知识。从为竞争力极强的媒体投资而精心设计的剧本，到直击广告科技的黑暗面。

资金用途

adChain 资金用途



发展蓝图

2017 年 6 月 – AdToken 发行
2017 年 8 月 – 注册表部署
2017 年 9 月 – 标头竞价点对点交易所
2017 年 10 月 – 启动去中心化应用程序赏金计划
2018 年 1 月 – 数据市场
2018 年 8 月 – 向所有代币持有者开放质疑注册表的权利
2019 年 2 月 – 实现完全去中心化，向所有代币持有者开放注册表应用程序

代币发行细节

经由 ConsenSys 和 MetaX 共同的好友，微软区块链领导者 Yorke Rhodes 介绍，两个组织展开了的合作已经持续了一年多。收到社区成员、行业参与者和法律顾问的反馈意见后，该平台本身在过去的六个月内历经多次迭代。在过去一年中，ConsenSys 和 MetaX 预售了 10%的代币，为后续开发和 DMA 及其成员组织等行业参与者提供资金，并支付法律分析费用。代币预售的参与者是那些希望看到 AdChain 平台在广告技术行业成为变革性协议的人。2017 年 6 月底预期公开发行 10 亿枚代币，所以 10%的预售代币是 1 亿枚。

代币细目如下：

- 公开发售 5 亿枚代币，募资上限为 1000 万美元。
- 根据下方的详细定时锁计划表，为 MetaX 保留 2 亿枚代币
- 根据下方的详细定时锁计划表，为 ConsenSys 保留 2 亿枚代币
- 通过多个预售协议（如上所述）出售 1 亿枚代币为资助开发

ConsenSys 和 MetaX 将协同履行本白皮书中概述的发展蓝图。 ConsenSys 和 MetaX 认为，在第一轮“代币发售”期间就公开发售近 75%的代币是十分不专业的行为。如果只进行一轮融资，那么一个正常创业公司的失效率将会变得很高。ConsenSys 和 MetaX 认为，随着时间推移逐渐发售代币是更好的选择，因为（1）AdChain 将会在数字广告业逐渐达到预设的里程碑;（2）ConsenSys 和 MetaX 将继续推动并发布 AdChain 协议的新进展。由此，ConsenSys 和 MetaX 认为，在第一次公开发售后，保留 40%的代币对该平台最为有利。这使得 AdChain 团队更为灵活，以便在必要时开启未来代币发售。

此外，ConsenSys 和 MetaX 认识到，公开发行代币会找到一批希望进一步了解他们所持代币功能的激励式参与者。因此，ConsenSys 和 MetaX 计划从 40%的保留代币中抽取一部分托管代币来为社区构建储备。一年以后，当 AdChain 协议中的治理方法更为具体化之时，ConsenSys 和 MetaX 计划托管这些代币，让代币持有人投票决定机制更改是否符合要求——这确保了 ConsenSys 和 MetaX 进一步减少对 AdChain 系统的中心化控制。

为了表明 ConsenSys 和 MetaX 对该系统的承诺，各实体已同意按以下解锁时间表锁定所有代币：

- 公开发售 1 年后解锁 50%
- 公开发售 18 个月后，解锁剩余代币

AdChain 未来工作计划

上述 AdChain 注册表和 TLS 验证机制都已经支持服务器端标头竞价，服务器端标头竞格意味着发行商或其代理直接从需求方得到投标申请，而无需通过中介交易所。独立于区块链的发展，服务器端标头竞标在广告技术上一直有一定影响，因为它为广告发行商提供了投标的透明化，并在供求关系中剔除了中间人。[8] 它适合引入 AdChain，因为它也是一种点对点科技，且与新兴数字货币领域中开始流行的各种设计模式相关联。妨碍整个行业采用标头竞价其中一个因素是“识别（discovery）”问题，即如何识别另一端发出入站报价请求的实体。AdChain 注册表在标头竞价的识别问题中作出了突破，收到报价的一方可以简单地通过 TLS 验证以及 AdChain 列表来确定该未知的实体是否有足够信誉。

我们的长远目标是将区块链和 AdChain 注册表的优势带给对于服务器端标头竞价不能满足需求的用户。随着网络不断去中心化，实现客户端标头竞价的识别将有非常大的需求，而支持多跳网络供应链中的认证将是构建完全程序化的特设供应链中的一次突破。使用区块链和内容寻址文件系统来验证广告标记的传递与显示能够消除一整类的广告欺诈。身份关联行为的强烈归属感可以说是网络广告的程序化中的一个难以达成的目标，如 uPort 这样的开放身份系统也许可以让它实现。

客户端标头竞价中的发现

类似于服务器端标头竞价，客户端标头竞价同样无需中间交易所，让广告行业的里供应商能够直接点对点进行交易。顾名思义，客户端标头竞价的请求源自浏览器而不是发行商控制的服务器。由于浏览器无法安全储存秘密，因此无法用双向 TLS 来验证浏览器发出请求时的需求。利用新兴的客户端签名标准来构建类似 AdChain 用户注册表，甚至在已有身份系统中用公开认证映像来实现该功能，这也许将变得可行。我们应该能够验证使用者，而不是验证发行商。

[8] “Envisioning The Future In A Server-Side Header Bidding World”. Rachel Parkin. AdExchanger. February 1, 2017.

深度供应链审计

AdChain 注册表允许广告主以注册者的身份，在一个干净的供应池里直接点对点来验证竞价者。在实际操作中，现在的多数广告交易都是在多跳供应链中进行的。我们使用相互 TLS 验证的方法对于在供应链中不直接相关联的两个实体并没有作用。也就是说，一方可以验证他们正在对话的个体，而不能验证该个体通过双向 TLS 正在代理的委托人（“我是 bar.net，我为 baz.net 服务而 baz.net 为 foo.net 服务）。实现该功能需要应用层认证逻辑的创新，涉及广告标记和签名打包的改变。

创作者验证

注册表可以让 AdChain 成员用来注册个人创意资产的哈希和元数据，其中元数据可以包含例如该创意媒体类型、其 IAB 内容分类法及其规模等内容。这份注册表可用于对整个供应链中的创作者进行主动验证，或允许发型商通过元数据将广告等级列入黑名单。

标签注册表跟踪

该注册表可以让分析数据供应商注册其 JavaScript 跟踪标签的一个哈希。这些标签用于追踪用户与网页上的广告的互动情况，但有时可能会被黑客侵入，在不知情用户上网时安装勒索软件。如果 AdChain 社区可以强制执行新的跟踪标签的审核流程，且发行商能够在运行前验证跟踪标签，那么恶意软件就难以通过广告扩散。

与身份相关操作的强归类性

互联网广告科技的核心是一个以需求为中心的归类协议以及可证明的表现量化工具。当广告主为效果而不是为曝光量付费时，一次曝光是人还是机器人导致的就不再重要；如果一次曝光导致了消费，那么广告主的最终目标就达成了。

总得来说，互联网广告的归类性是很低质量的。除非是一次点击导致了最终购买，我们难量化一次广告曝光是否真正有效。即使点击导致了购买，我们也很难将购买的功劳都归功于这次广告曝光，因为可能用户已经多次在其他网站看到了该产品的广告最终才导致了购买。广告主根本无法了解他们的努力是否有效，同时广告发行商也拒绝提供相关信息，因为显然以曝光量出售广告比以效果出售广告更有利可图。

Cookie 同步以及其他所有广告业的黑科技都没有为如今的开放式网络提供一个可靠的归属科技。在区块链上运行的开放式身份系统有机会通过封闭式的社交媒体平台提供的大量可靠数据来打造一个建立在开放互联网上的高效归类系统。

先进的投票和治理系统

AdToken 持有者可以直接通过投票参与是否将申请人列入 AdChain 注册表的流程。如果能为 AdToken 持有者赋能，让他们可以将投票权交给智能合约，例如 Gnosis 的预测市场或者可靠的代表人，那么我们就可以拥有一个类似于 PoW 矿池一样的可靠投票系统。

另一个可以探索的方向是将被锁定的代币运用到投票中，这个系统被 Vitalik Buterin 和其他人讨论过。[9]将被锁定的代币运用到投票系统可以提高 AdChain 社区投票者的利益相关性，因为只有在一定时间框架后那些投票者才能成功退出。

曝光跟踪

除了帮助发现点对点表头竞价，AdChain 也可以被延展到其他的功能，例如一个接近实时的曝光追踪统计工具。传统的广告合约有一个 30-60 天的结算周期，所以不同方对于曝光量的不同统计在合约结算前很难统一。曝光跟踪统计的差异同差可以高达 20%。[10]这些差异部分是来自于浏览器和网络之间存在的一些固有问题，例如延迟、网络链接失败、广告阻拦插件和不同服务器之间的垃圾信息过滤技术。这种在行业间被广泛理解的差异却常被利用来欺骗广告主，通过欺骗性数据和谎报曝光量。

通过实现安全链下及时、私密、零消耗交易的状态通道技术，广告曝光可以在各个节点之间被实时同步，避免了潜在的欺诈行为。利用通道技术来追踪广告曝光的原型已经完成，这个原型的代码和文档可以在 GitHub 上被浏览：https://github.com/adChain/AdMarket。一旦被部署，这将是第一个实现工程应用的状态通道技术实现，同时它会在整个网络上运行，有能力处理每天过亿的曝光记录，同时通过基于以太坊的只能合约来保证安全。

小额支付和一个真正的三方广告市场

如上所述，第一个 AdMarket 实现会主要用来进行统计；真正的支付会通过传统银行进行。同时，AdMarket 状体通道实现会转换到一个真正的小额支付系统。在这个系统中，广告主会对广告发行商的每一次曝光都进行一笔小额支付，并周期性地在链上结算。.

通过以太坊钱包浏览器插件，例如 MetaMask，用户可以参与到这个广告市场中。他们可以选择自动支付网站的广告发行商一定的合理的费用，从而让整个网站变得没有广告。未来，如果用户选择不屏蔽广告，那么广告发行商可以选择与用户共享广告费用。

---

9 "On Coin-lock voting, Futarchy and Optimal Decentralized Governance". Vitalik Buterin. Reddit. 2016.

10 "Third-party discrepancies". Google DoubleClick.

实时数据流

AdChain 协议可以被延展基于状态通道技术的微支付，辅助发现和购买用户广告参与度的实时数据流。这些数据可以被捕捉到这些数据的广告主或者广告发行商出售，甚至未来可以被用户自己出售。用户通过以太坊钱包浏览器插件可以轻松地捕捉到自己的数据流，然后选择性出售与用户身份链接的认证数据流给数据分析商、广告研究组织、中间商或者其他人。