DMChain

基于区块链的去中心化数字广告平台

白皮书

3.0

DMChain

目录

DMChain

DMChain

目录

DMChain

免责声明

本文件仅作提供信息之目的，不构成要约或请求销售ADE代币或任何相关公司的股份或证券。 任何要约或请求仅可根据所有适用的证券及其他法律，通过提供备忘录作出。

这份中文白皮书是有关DMChain的主要官方信息来源。如有必要，DMChain基金会保留对本文档进行更改和编辑的权利。您应确保您已阅读和理解白皮书的最新版本内容。

本白皮书的目的是向潜在未来用户介绍DMChain及其相关产品解决方案，下面列出的信息可能并非详尽无遗，也不代表着任何合同关系。该文件的唯一目的是向潜在的用户提供相关和合理的信息，以便他们决定是否进行深入的分析和参与的服务乃至使用。

ADE代币是实用功能代币。本产品不是数字货币，证券，商品或任何其他类型的金融工具。ADE代币不能用于本白皮书所涉及之外的任何目的，包括但不限于任何形式的投资，投机行为或其他财务目的。DMChain基金会将不承担因使用者进行盈利为目的的DMC代币交易而为其带来的任何损失。

DMChain不是一个金融产品。此首次代币发行不是任何方式或形式金融服务，它也不是任何股权。它是为了交易零售社区的利益品。ADE代币仅是一种进行交易的方法。他们不应该因信仰，假设或判定其有升值的可能性而将其和其他有价值物品互换。请在作出决定之前仔细阅读白皮书的最新版本内容。您对您的加密货币全权负责。它是为了交易零售社区的利益而创建的软件产品。ADE代币确实是一种在DMChain上进行交易并获得额外折扣优惠的方法。他们不应该因其信仰，假设或可能增加价值的其他价值项目而被交易。请在作出决定之前进行调研。

免责声明

ADE代币不适用于在任何可能禁止销售或使用数字货币的司法辖区内进行销售或使用。ADE代币不以任何形式赋予任何其他权利，包括但不限于任何所有权、分配（包括但不限于利润）、赎回、清算、所有权（包括所有形式的知识产权）或其他财务或法定权利，白皮书中具体描述的权利除外。

本白皮书中包含的某些声明，估算财务信息被视为前瞻性声明和信息。而这些有关ADE代币当下的期许对未来的展望是DMChain基金会根据对目前态势的考量和预测和财务市场的市场趋势得出的。

除非另有说明，否则本白皮书中关于DMChain或ADE代币未来业务活动，业绩或盈利能力的所有声明和信息均被视为前瞻性声明。这些前瞻性陈述只是DMChain目标性的陈述，并不是对未来经营业绩的预测或预估。本白皮书中包含的前瞻性声明基于DMChain基金会认为合理的假设，但DMChain基金会不保证这些前瞻性声明是完全准确的，并且由于DMChain基金会管控能力范围之外的因素的存在，这些前瞻性声明的结果可能与最初的预期有所偏差，包括TGE的实施程度，市场条件的变化和/或可能影响DMChain运营的法律和监管变化。

摘要

DMChain

随着互联网行业流量红利消失，导致数字营销市场规模增速放缓。互联网广告市场成熟，无论是增速还是市场结构进一步趋于稳定，未来行业需要通过寻找具有发展潜力的细分市场，进行大规模的商业化变现。一方面是基于现有存量市场的效率提升，加速展示广告在程序化交易模式的改造，营销价值最大化变现。另一方面，在内容营销、信息流广告等新的营销方式探索方面，以库存增长拉动市场向前发展。

程序化购买作为展示广告的一种重要交易模式极大地提升了市场各方的流量交易效率，受到市场各方认可，多种类型厂商涌入市场。然而，正如约翰·沃纳梅克——第一个投放现代广告的商人——所说：“我知道我的广告费有一半浪费了，但遗憾的是，我不知道是哪一半被浪费了。”广告行业的不可统计性与广告欺诈问题由来已久，一直得不到有效的解决。区块链技术的出现有机会让这个困扰广告行业的“黑箱”问题得以有效解决。

DMChain——一个去中心化的数字广告系统，是在基于区块链技术的基础上利用大数据与人工智能技术对现有的数字广告行业的颠覆性改造。

DMChain具有如下特点和优势：

- 没有数据欺诈的真实流量
- 性价比更高的偏平化广告投放方式
- 公开透明的程序化投放、可信的自动结算
- 更真实、更精准的数据统计，更有效的触达受众
- 为广告业内所有不同的参与者带来更多价值

摘要

DMChain

而从基础建构设计上DMChain也利用第三代区块链平台Cardano（ADA）加快产品的迅速落地。我们为DMChain生态系统设计了四大产品模块：

DMNetwork、DMExchange、DMID、DMBAAS，希望用区块链彻底的改造广告行业。

- DMNetwork——基于Cardano设计开发的区块链网络，让媒体主（Publishers）可以把广告位上链，使每次的展示、每个点击的公开透明可信。

- DMExchange——基于Ouroboros共识算法的去中心化广告交易平台，基于DMNetwork的数据支持，让广告主（Advertisers）的投放广告价格不再是黑匣子。

- DMID——区块链世界广告受众的统一账号，通过Token 经济生态，让每个人的数据都重新获得价值。在不侵犯用户个人隐私的前提下，通过分析生态内收集到的数据，提取受众群体的偏好和行为模式，以及不同类别媒体主的群体特征，并通过 DMData API与生态外的数据需求方进行交互，为整个生态带来额外的经济收益。

- DMBAAS——基于区块链可信数据打造的广告程序化投放服务系统，为广告商（Agency）提供更好用的投放工具。同时也为媒体主（Publishers）提供更多基于区块链技术上价值变现的创新。

项目概述

市场概况

2017年，整个数字广告行业的总收入达到了5630亿美元。根据AOL和Millennial Media的一项研究显示，Google和Facebook作为业内两个最大的广告发布商，瓜分市场总收入的57.6%。巨头发行商在目前的数字广告行业中占据统治地位。

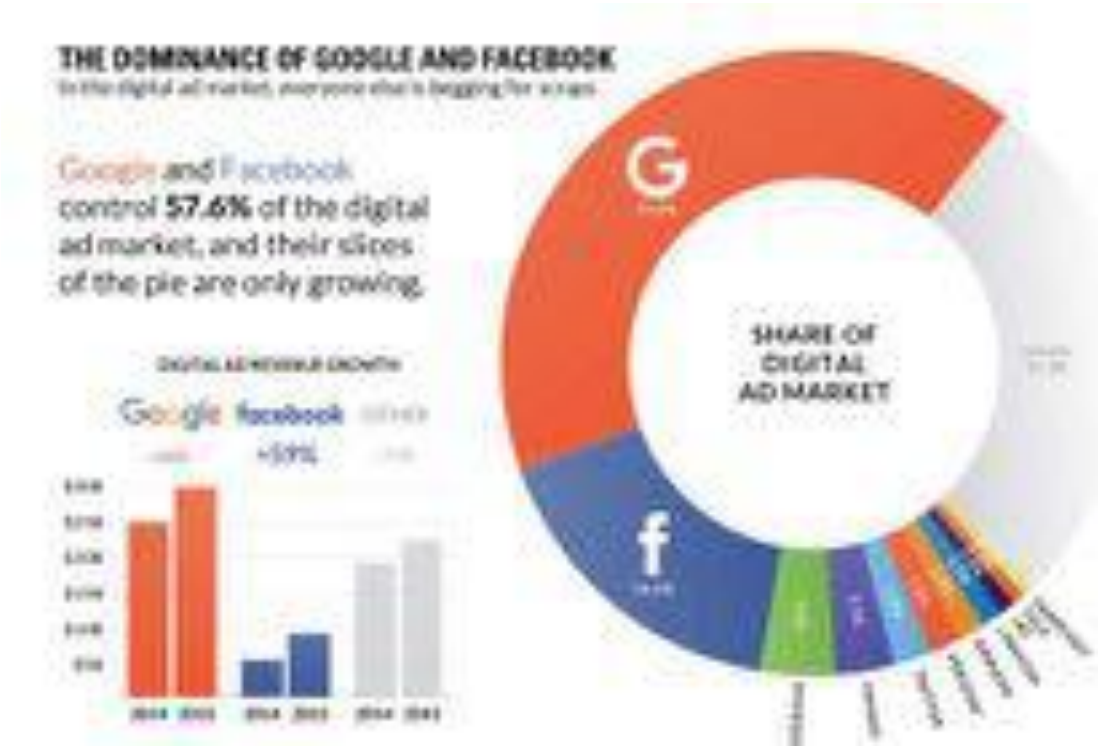

图 1. 数字广告市场占有率

展望整个广告行业的发展趋势，数字广告的发展速度仍旧快于传统的电视广告。移动终端将会很快成为最大的广告分发渠道，在此渠道发放的各种类型的广告中，视频类的广告保持着最快的增长速度。举例来说，Youtube 依靠每月处理的30亿次搜索的数量，已经成为全世界第二大的搜

DMChain

索引擎。在18–34的年龄段，它比美国的任何一家有线电视网络覆盖到的受众都多。根据一项由 BI Intelligence Estimates, Magna Global, IDC 和 IAB 的联合调研，在各种广告形态中，与 DMChain愿景密切相关的由程序投放的广告的占比，由2013年的31%增长到了2018年的50%，并且还在持续增长。

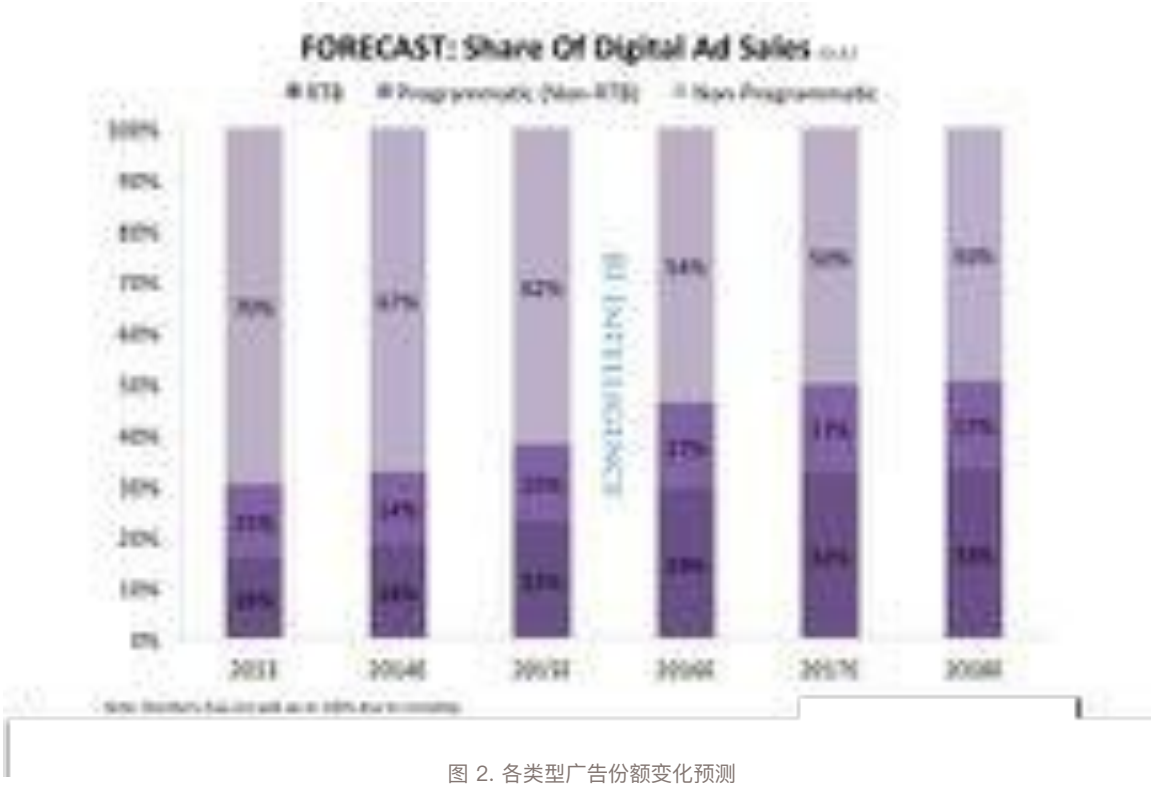

图 2. 各类型广告份额变化预测

问题和挑战

当整个行业构建在一个缺乏信任机制的平台上时，广告欺诈的数量必然随着整体产业的发展而显著增加。广告欺诈这个在行业中存在已久的问题，不仅从负面影响了广告主的成本预算，也进一步加重了行业中各个参与方相互不信任的问题。根据 WPP GroupM的一项研究，广告欺诈消耗了全球数字广告营销预算中的20%，这部分预算也被称为“信任成本”。Talkingdata 的一份2017年移动广告产业报告中给出了更加具体的案例。报告中称 iOS 已成为广告欺诈的重灾区，作为衡量广告主整体支出的重要指标的点击数，仅在2017年就增长了17.8倍（在iOS平台用户基数没有发生剧烈变化的前提下）。

DMChain

广告欺诈的严重已经到了不能放任的程度。在消除其负面影响方面，我们相信即使传统的反欺诈方案仍在不断进化，区块链凭借其去中心化和智能合约的特性，仍然是这个问题天然的最优解。一个建立在区块链生态上的数字广告产业必将是更加开放和健康的。

中介成本

作为一个高度发达的产业，广告业已经拥有了成熟的供应链体系，其中包括多层次的代理体系。代理机构主要负责匹配广告客户和广告发行商，他们会从中收取巨额的手续费。这给广告主和发行商都增加了很大的负担。此外，为了找到合适的广告发行商，广告主通常要面对的是一个很长的产业链，其中包括：广告代理商、媒体购买者、营销商、联属网络商等。这些错综繁杂的代理机构使得广告业的价值交换变得非常低效。

通过在区块链上建立广告生态系统，上述这些信息不对称将会被消除，因此支付给中介机构的成本将被降到最低。

尾部媒体主变现困难

与顶级媒体和大型发行商不同，小型媒体主在传统广告生态系统中一般很难变现。因为大部分广告预算都被那些大发行商所占据。因此，中小发行商在增加收入方面面临的选择非常有限。他们既无法支付昂贵的代理费，也无法负担一个强大的销售团队。

借助区块链技术，中小型发行商现在可以通过“代币化经济”在更多元化的环境中调动社区的力量以提高他们的收入。

图5. 部分数字广告媒体主

效率低下

在数字广告市场稳步发展的同时，反广告技术也在不断发展。像Adblock这样的工具已经被广泛使用。这些反广告商在浏览器上大量屏蔽广告，使得发行商的收入被极大降低。

与此同时，广告投放的结果和反馈缺少一种统一的衡量方法。在衡量广告效率时，广告主在大多数情况下只能依赖来自机构或第三方的数据和分析。由于这些数据缺乏透明度，数据收集方式分散，广告主通常难以得到准确的答案。

最后一点，代理商和广告主都只能根据自己的数据库信息来寻找他们认为最理想的发行商。但是，收集这些数据也是一项艰巨的挑战。在整个行业中，没有任何一个参与者可以拥有全部的数据，因为他们都在以自己的方式从他们所掌握的用户中收集片面的数据。这造成了一种混乱的局面：行业里的各方通常不会也不能分享他们的数据，而且没有人能够得出完整和精确的用户画像。

解决之道 —— DMChain

图6. DMChain连接所有媒体主，广告商，广告主和消费者

DMChain能够解决上述的所有问题。DMChain建立在Cardano（ADA）之上，它利用智能合约和数据透明度，为广告业者提供了一种解决方案，无论广告主的规模如何，均可确保交易的安全性、可验证性、可追溯性和易用性。此外，它还消除了广告行业的不信任性和不确定性，并为广告主提供了更明确的市场目标，以及可跟踪和可量化的广告投放结果。

DMChain的参与方可以访问区块链上所记录的全部数据，并结合深度学习和数据挖掘技术，描绘出更完整，更精确的用户需求，同时制定出一个反欺诈机制。

此外，为了确保广告在不同市场中的合法性和有效性，DMChain还弱化了一些中介机构的功能，并在生态系统中引入了叫做审查者的第三方。这些审查者可以通过参与预估各支广告在各个市场的合规状况及受欢迎程度获得奖励。

DMChain

的特点和优势

- 没有数据欺诈的真实流量
- 性价比更高的扁平化广告投放方式
- 公开透明的程序化投放、可信的自动结算
- 更真实、更精准的数据统计，更有效的触达受众
- 为广告业内所有不同的参与者带来更多价值

DMChain

愿景

为广告业者构建更透明的交易渠道

广告业者可以通过DMChain找到与自己产品目标相匹配的客户。广告商能够更好地了解他们的客户，并提供合适的产品和服务。

通过公平的定价方式增加发行商的收益

随着区块链技术的不断发展，广告产业的产品关系也在发生着变化。行业巨头将无法垄断整个行业。通过使用区块链上的实际数据，发行商将会重新掌握定价权。代币化经济为发行商提供了更多的货币化渠道。

获得更多广告受众的关注

在互联网时代，用户数据是大多数互联网公司盈利的重要来源。但是，用户数据的价值却没有得到应有的重视。我们认为，一部分中介成本应该用于奖励那些愿意花时间观看广告的观众。通过区块链技术，我们可以将用户数据反馈给行业从业者，并根据用户的需求对症下药。

提高代理商的效率和透明度

代理商作为广告行业不可或缺的一部分，有着自己独特的价值。由于目前高度集中的互联网商业模式，信息和价值变得非常不对称。我们希望通过区块链技术打破这种行业潜规则。价值信息将变得更加透明，交易过程也将变得更加有效。

DMChain生态

DMChain生态引入了 ADE Token 代币作为生态内价值交换的载体， 整个生态由DMNetwork、DMExchange、DMID、DMBAAS四个部分构成。

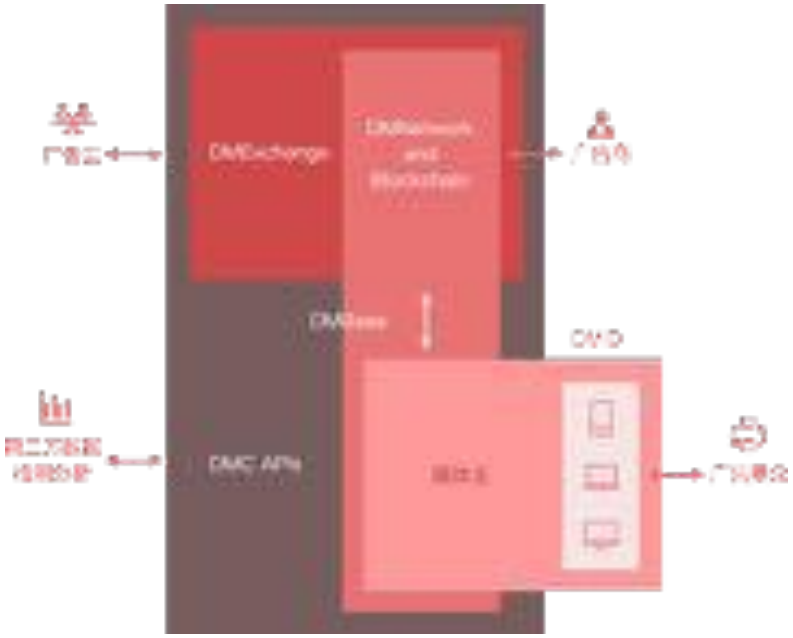

图7. DMChain生态

架构模块介绍

ADE Token

ADE Token可以在 Cardano 公链上自由交易兑换。作为 DMChain 生态内的价值载体，ADE Token 系统内的所有交易均以 **ADE Token** 结算。具体的交易和结算场景包括但不仅限于:

- 广告主在广告完成展示后，使用 ADE Token 向媒体主进行支付。

- 当整个流程有广告商参与时，广告主使用 ADE Token 向广告商进行支付，广告商使用 ADE Token 向媒体主进行支付。
- 广告主展示包含注视奖励的广告时，当受众观看广告或与广告发生互动后，广告主使用 ADE Token 向获得奖励的受众进行支付。
- 外部的数据需求方使用 ADE Token 从 DMChain 系统中购买数据。
- 广告受众完成真实身份认证后从系统中以 ADE Token 的形式获得奖励。

DMNetwork

DMNetwork承载着系统的核心算法及智能合约，它将广告主、发行商和代理商连接在一起，记录他们之间活动产生的各种数据，包括交易记录，消费行为，发行商的历史活动和声誉等。
DMNetwork主要基于ouroboros 机制，发行商可以通过API将他们的广告资源上传到DMNetwork。由于发行商的影响力和历史表现可以通过关联的 DMID 进行追溯查询，这确保了每个广告样品的透明度和可信度。

DMExchange

DMChain主链上的去中心化广告交易系统：媒体主们把通过SDK上链的广告位（流量资源）写在智能合约中，广告主（Advertisers）与广告商（Agency）按需采购。得益于ouroboros的共识机制高速处理能力，广告位的竞价交易可以做到RTB（Real Time Bidding）。

DMID

DMID是广告受众区块链账户统一标识。它被用来管理和统一用户在链上和链下的个人数据。DMID在生态内用于匿名地关联用户浏览偏好和行为模式，媒体主在不同细分领域内的表现声望，以及广告主的历史投入记录等。这些由 DMID 关联的透明化储存的数据是整个生态的基础。在生态外，DMID 作为打通链上

和链下的接口，用户可以选择有偿地授权 DMChain 导入他们在其他平台上的数据信息以丰富他们的用户画像，广告主和媒体主利用这些额外的用户数据将能够做到更加精确的匹配。作为回报，这些用户将获得ADE 代币。

个人信息认证激励机制（Proof Of Real Flow / PORF）

为了获得更多真实准确的数据，DMChain以DMID为载体，引入了PORF（Proof Of Real Flow 真实网络流量证明）作为激励受众认证真实用户信息的机制。

为确认受众的真实性，受众需要进行KYC实名认证。认证方式包括一次性提供身份证、护照等身份文档进行实名认证，以及周期性重复授权关联第三方服务账号等。身份认证信息经过加密后保存在DMID中。用户通过认证后可以获得算力——算力越高的用户在同一单位时间内获得ADE的数量会越多。认证多种信息所获得的算力可以叠加。由于第三方的授权关联通常具有一定的有效期，当已关联的第三方用户信息过期失效时，相应的算力将会被扣除，用户可以选择再次授权关联其第三方的账户信息来恢复对应的算力。

ADE在铸币和发行阶段将保留大量的预留代币用于回馈对整个生态有所贡献的参与者，提供真实认证信息的用户群体正是主要的回馈对象之一。这些预留代币会通过预定的算法按计划持续缓慢地释放直到2140年完全释放完毕。在那之后，社区已达到高度成熟和去中心化，每一次广告投放的交易费用都将包含着审核者和广告受众等贡献者的回报。当用户通过APP、API、浏览器插件等方式在DMChain上保持在线时，系统会将当前正在释放的预留代币，按当前在线的用户能力值总和按比例获回馈给用户。

DMBaas

DMBaas是为广告主、广告商、媒体主服务的SAAS系统。DMBass是DMChain上的程序化广告系统。它为广告主，代理商提供了更好的广告工具。同时，也为区块链上的媒体主提供了更多的获利方式。通过使用SDK或插件，DMChain

还可以与媒体主的终端用户进行数据交换，数据需求者也可以自行购买匿名的用户数据。DMBass主要包括以下模块：

图8. DMBaas

DMSSP：为媒体主提供的基于区块链的供给方平台，供给方可以看到相应广告位的实时收益情况并实时结算。**并可为优质流量资源提供如TGE等服务。**

DMDSP：为广告主提供的基于Cardano的采购方平台，采购方可以通过DMDSP直接程序化投放。DMChain会通过去中心化的广告审核机制对广告内容进行审核。通过审核的广告内容会存储在IPFS上，并一同写入DMChain。采购方还可以通过Dashboard观察到广告投放的情况并作出实时处理。

DMDMP：为媒体主、广告主、广告商、第三方数据需求方等提供的基于区块链可信数据的数据分析挖掘平台。

角色介绍

广告主 (Advertiser)： 通常是持有预算，准备通过数字广告的方式为自己的产品或服务做推广的公司或组织。在 DMChain 的生态中，广告主将会有更多的数据参考，以及算法辅助，来帮助他们直接联系到最合适的媒体主。

媒体主 (Publisher)： 通常是媒体组织或者有较大公众影响力的个人，在 DMChain 的生态中，媒体主无论规模大小都可以通过智能合约和 DMExchange匹配到适合自己的广告主，实现快速变现。

广告受众 (Audience)： 普通的广告观众。在 DMChain 的生态中，他们在点击观看广告的同时可以将自己的注视变现，依照智能合约获得相应的代币奖励作为回报。受众还可以通过 DMID 关联其生态外的其他账户，授权DMChain 导入外部账户的信息，根据PORF（Proof Of Real Flow 真实网络流量证明）算法 获取相应的代币奖励作为回报。

审查员 (Reviewer)： 审查员是 DMChain 中独有的功能性角色，审查员同时可以是持有ADE代币的普通受众。审查员可以在系统中参与去中心化的审查，对一则广告是否应该投放给出一个群体建议。审查员最明显的作用是可以显著减少点击诈骗，其次当比较大的广告主为相同的产品或服务在不同地区投放广告时，审查员可以参与评估广告在各个地区的合法性和潜在效果，保证广告的质量和成功率。

以下介绍DMChain对于广告内容审查的算法：内容审核权益证明/ Content Check Proof of Stake / CPoS

为实行去中心化广告内容审核，避免中心化舞弊，在广告内容上架前需要通过内容审查智能合约的审定。广告商需要向智能合约存储一定量的ADE代币以启

动广告审核。持币者要成为内容审查员，必须先行向智能合约抵押一定数量的代币，抵押数量越高，被智能合约选中成为审核员的几率越高。随后智能合约将随机选取21名审核员对广告内容进行选举。被选中的审核员需要在1小时内给出审核结果否则将失去抵押代币。当超过21名审核员给出审核结果，智能合约将自动对审核员做出奖惩。奖惩方式如下：

–如果超过2/3的审核员认为审核通过，则该广告则可进入投放。此时，认为不通过的审核员的抵押代币将被扣除并与广告商存入智能合约的代币一起平分给认为通过的审核员。

–如果超过2/3的审核员认为审核不通过，则该广告则不予投放。此时，认为通过的审核员的抵押代币将被扣除并与广告商存入智能合约的代币一起平分给认为不通过的审核员。

–其他情况，广告商存入智能合约的代币将平均分配给审核结果为多数审核员认定结果的审核员，而给出非多数审核员认定结果的审核员的抵押代币不会失去。

数据需求方 (Data Demander)：数据需求方是跟 DMChain 系统有密切互动的第三方角色，他们一般是对系统内各角色群体的属性，偏好或者行为模式感兴趣的公司。他们会使用 ADE 代币通过 DMData API的接口来购买和使用生态系统内产生和提取的数据，为生态系统带来额外的收入。

图9. DMChain各角色及代币流转图示

生态场景

以下我们通过一个典型的端到端的案例来阐述生态中各个模块的作用，以及各个角色之间的互动关系：

图9. DMChain各角色及代币流转图示

媒体主 P (Publisher) 是一家擅长经营电影和音乐相关内容的自媒体，他生产的内容通过生态内的若干视频和文字渠道影响着两类广告受众 F(Film Fans) 和 M(Music Fans)。

系统可以对 P (Publisher) 的历史受众的用户画像进行整体分析，于是广告主 FA (Film Advertiser) 和 MA (Music Advertiser) 都可以比较容易的获得 P 的受众会对自己的产品感兴趣的信息。由于P 曾经合作过的广告主的 DMID和他们的支付记录，P 的历史内容浏览数，历史广告的互动数，以及影响受众数量都可以用过P 的 DMID 进行查询，在竞价投放之前，FA 和 MA对在 P 的平台投放广告的成本和效果已经有很清楚的预判。

当 P 将通过 **DMNetwork** 的 SDK 将自己的广告位上链放置在 DMDSP 时，FA 和 MA 开始了跟其他广告主的竞价，并最终竞价成功触发了智能合约中的状态转换条件。他们分别获得了在 P 的渠道上播放自己广告的部分时间。

FA和 MA 将自己的广告播放之前，系统会根据两支广告的类别选中的部分审查员 **R(Reviewer)**，R 会对 FA和 MA 的广告进行审查和预估。FA和 MA 得到群体审查的正面反馈后正式将广告投放并成功部署，做出与结果一致判断的 R 将根据智能合约中的条款获得相应代币奖励和声望奖励。

DMChain生态

DMChain

广告被部署投放后，当受众F(Film Fans) 和 M(Music Fans)开始消费 P 的内容时，系统会根据受众的 DMID 所对应的用户画像来准确判断该受众对FA和MA中哪一家广告主的广告更感兴趣，并成功展示出效果更好的那支广告。

当受众注意到广告，并与广告进行互动（有可能是一定数量的受众互动一定次数）之后，智能合约中的部分条件再次被成功触发。假设播放的广告是针对电影爱好者 F(Film Fans) 受众的，DMExchange 将会从广告主 FA (Film Advertiser) 的代币地址中按照事先完成的竞价自动发起一笔转账到 P 的地址中。而与这支广告互动过的受众也会根据智能合约通过 DMExchange 得到相应的代币奖励。所有这这些交易和互动的记录会被记录在 DMNetwork 的区块链上。广告主 FA 和媒体主 P 都可以实时的看到关于他们广告的实时数据统计。

当有音乐爱好者M访问到 P 的内容时，系统也会成功的播放 MA (Music Advertiser) 的广告，并完成相同的记录和结算流程。

通过上面的场景阐述，我们展示了 DMChain 是如何成功解决**潜在的点击诈骗，高额的中间商成本，尾部媒体主变现困难，广告效果难以预测**，以及**数据难以统一收集**等一系列问题的。

社区建设

DMChain 社区目前已有成熟的数字营销平台数字镭**DMLei**（www.dmlei.com）以及区块链及数字货币领域首家人工智能媒体平台**OKZ**（www.okz.com）加入，作为DMChain社区首批核心合作伙伴。

数字镭DMLei (www.dmlei.com)是面向中小企业的数字营销推广服务平台，曾获得小米系及阿里系的高管投资。DMLei平台目前已经聚合数万媒体主和广告主资源，通过智能 SAAS+人工服务的方式，提供一站式数字营销服务。

DMChain将基于 DMLei积累的资源和运营经验，致力于将 DMLei 向区块链的方向演进，打造出基于DMChain的全新社区。DMLei 平台上的数以万计媒体主和广告主顺利迁移到 DMChain 生态后，将会极大的繁荣 DMChain的社区，成为 DMChain 生态体系最早的参与者。

DMChain生态

DMChain

OKZ(ww.okz.com)区块链行业最全面最有影响力的全媒体资讯服务平台之一。

OKZ将作为首个接入DMID的区块链媒体，为DMChain上广告受众提供**区块链账户统一标识。接入的DMID的用户将获得**更加精确的内容推送。用户将获得ADE 代币作为回报。

技术解决方案和架构

DMChain技术生态系统

DMChain生态系统基于Cardano（ADA）的区块链和智能合约技术构建。利用状态通道和安全的去中心化数据存储所创建的多功能基础架构，可以在很高的广告交易并发下可靠工作。

具体来说，DMChain生态系统包括DMNetwork、DMChain两个关键组件，其中承载了防欺诈机器学习系统、数据加密等大量中间件。在以下的章节中，我们将详细解释DMChain区块链生态系统的技术设计和实现。

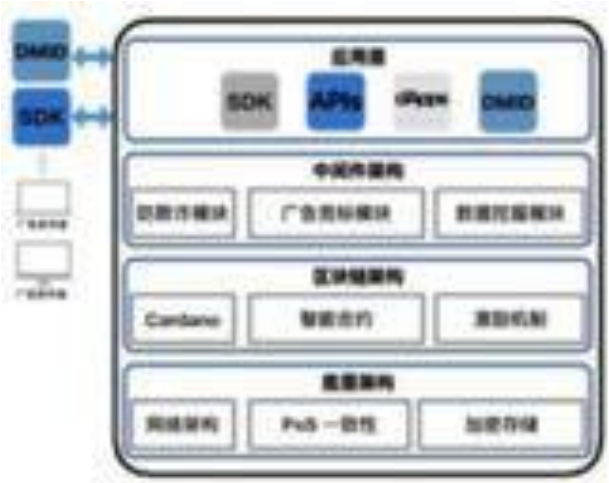

图9. DMChain整体模块架构

DMChain的区块链基础架构层

区块链技术从2009年中本聪发布比特币白皮书之后便开始蓬勃发展，到目前为止，市面上能见到数千种区块链架构。而这些架构的技术可行性及成熟程度参差不齐，导致区块链技术发展呈现一定的混乱。总体而言，区块链发展到目前为止经历了三个阶段。首先，比特币 [1] 作为第一代区块链技术开创性的解决了分布式系统中存在的信任问题。由于 **比特币** 采用工作证明（PoW）的方式来验证区块的有效性，矿工之间相互竞争区块打包的任务从而得到比特币作为奖励，而随着矿工参与者越来越多以及挖矿设备从CPU到GPU以及ASIC矿机的升级，挖矿成本逐年升高但是比特币区块链的交易性能并没有多少改观，因为比特币的区块时间是预先设定为十分钟的。为了提高区块链的交易吞吐量，**以太坊（Ethereum）**[2] 为代表的第二代区块链技术通常降低了区块生成的时间。现阶段以太坊的区块时间大约为15秒，交易吞吐量相比比特币区块链有较大的提升。同时，以太坊还引入了图灵完备的编程语言用来支持智能合约技术。然而，因为以太坊延续了第一代区块链技术的工作证明机制，以太坊区块链也经常出现大量交易无法及时被处理的情况。为了从根本上解决这一问题，以**卡尔达诺（Cardano）**[3] 为代表的第三代区块链技术开创性的提出权益证明（PoS）机制来保障交易的可扩展性，可持续性以及互操作/互通性。

随着区块链技术的快速发展，新的应用类区块链不需要从头开始开发底层架构，而只需要选择合适的底层链作为基础架构并在其基础上搭建应用层即可。鉴于DMChain对交易的高吞吐量、高可靠性以及高实时性的要求，我们采用更高效的PoS底层架构。另外由于**卡尔达诺（Cardano）**的安全性及可靠性在同类技术中处于领先地位，我们选择**卡尔达诺（Cardano）**作为DMChain的区块链基础设施。

卡尔达诺（Cardano/ADA）

卡尔达诺从2015年即开始研究及开发工作，其发起者Charles Hoskinson为以太坊的联合创始人，并有多个区块链项目的架构经验。卡尔达诺的权益证明算法名为**乌洛波罗斯**（Ouroboros），它决定了各个节点如何达成网络的一致性。乌洛波罗斯是第一个具有科学凭证其安全性的权益证明协议，它消除了需求能量消耗高昂的工作量证明协议而成功消除了区块链长久以来无法扩大应用的障碍。在工作量证明中，矿工投入运算能力来竞争获得生成下一个区块的权力并赢得奖励。相比之下在权益证明中，每个股权(Stake) 持股者都有被随机选取组成下一个区块的领导者，而被选取的机率与股权者拥有之股权比例成正比。为了确保区块链的安全性，选择股权者来制作区块的方法必须是真正随机的。为了产生领导者选举过程的随机性，乌洛波罗斯的创新是通过安全、多方执行掷硬币协议来达成一致。

卡尔达诺（Cardano）给DMChain主要带来三个方面的优势：

1. **可扩展性：**卡尔达诺可以带来极高的每秒处理交易量。因为DMChain上的应用会涉及到高频率的交易操作，要想实现高速交易，目前只有卡尔达诺可以支持每秒处理大量交易的能力。另外，由于区块链存在于点对点网络中，网络中的每一个节点都会有新生成交易的副本。如果每秒有上千万次或者更高的交易量，网络中的每个节点都需要大量的带宽来下载增量更新而导致不易扩展。为此，**卡尔达诺通过RINA（Recursive InterNetwork Architecture递归互联网架构）**的技术来解决这个问题。在RINA网络中每个节点都归属于某个子网并能与其他网络在需要时进行通信。对于不断增长的区块链存储所有发生的事务，卡尔达诺通过修剪、压缩及分区等技术进行解决。

2. **可持续性：**现在很多公司希望做与区块链及加密货币相关的业务，并通过ICO为公司筹集资金。但是随着大量ICO丑闻的爆出以及过度投机，ICO并未能为多少公司的业务、技术和产品带来大的提升。因此，只是为了筹钱的ICO没有

持续性，而卡尔达诺建立了**金库（Treasure）**机制，这个金库本身不受任何人控制，并作为一个智能合约存在，任何可以改进卡尔达诺协议及应用的个人和公司就可从该金库中获得部分资金。这种金库机制可以利用持续的现金流来保证卡尔达诺生态系统的可持续性。

3. **互操作性：**由于现在上千种区块链和数字货币并不互通，跨链转账当前并不可行。卡尔达诺的愿景是成为区块链的互联网，这样资产就可以在各种区块链之间转移。通过将交易元数据与交易绑定，从而解决跨链转账的难题甚至实现数字货币与法币的无缝转移。同时，由于卡尔达诺支持**侧链**技术，DMChain可以在此侧链架构下实现代码和数据的独立性，减小主链的负担而避免数据过度膨胀，实现自然的分片。

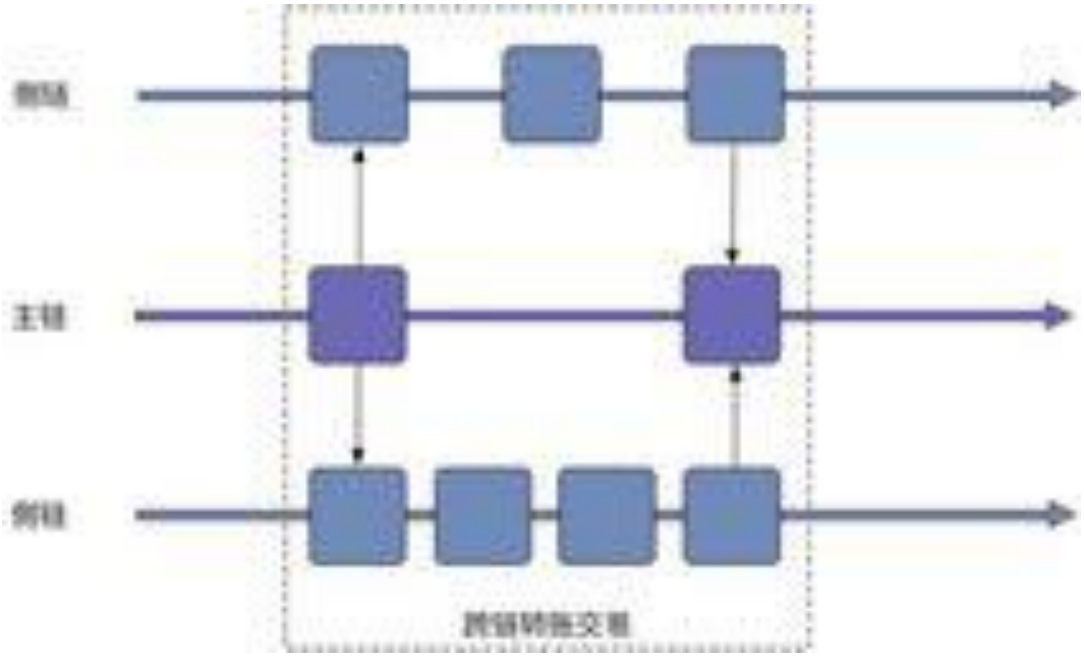

图10. 跨链交易行为

卡尔达诺对**侧链**技术的支持也可以支持DMChain的多种业务场景，从而减小数据在主链上的存储量，进而减小运营成本。例如，DMChain可以将广告生态中的大部分内部交易转移至侧链上执行，在执行完成之后再将结果同步至主链。

除了降低成本，这种操作还可以提高业务场景的灵活度，因为在侧链上我们可以为不同的场景制定不同的区块同步时间，以方便业务逻辑的及时执行。

智能合约

数字广告系统中的很多应用场景都是天然的智能合约，比如，当一个广告的投放次数达事先协定的数值之后，广告主就需要支付给广告投放者一定的价钱。这些场景可以用智能合约实现，从而实现商业逻辑的自动化运行。在法律系统中，在许多情况下这些协定具有法律约束力，不要求形成一个完备的协议。但是在智能合约系统中，由于合约的执行者是参与区块链的机器节点，而这些节点在大多数情况下都不能理解这些商业逻辑。因此，DMChain需要提供一种形式化的工具将商业逻辑形式化，形成一个能自主在区块链上运行的程序。

由于现在通用的智能合约系统提供了一套有限操作指令集用来支持智能合约的执行，同时为了方便合约的撰写，这些系统还在此基础上提供一套图灵完备的高级语言方便用户将实际的业务逻辑编译成机器可以理解和执行的操作码流程。例如基于以太坊的Solidity语言以及卡尔达诺的Plutus。

为了更高效的将业务逻辑转换成机器可以理解和执行的字节码，**DMChain还提供一个领域专用语言（Domain Specific Language，DSL）[4]** 供用户使用。这个DSL在图灵完备的高级智能合约编程语言基础上进行更高层级的抽象和封装，可以让普通用户以可见即所得的方式进行查阅、编辑和编译成最终可执行形式。同时，用户也可以使用这个功能对智能合约进行模拟运行，而不用将其部署在实际的区块链之上从而缩短智能合约的撰写时间并有效降低合约的开发成本。

除了降低成本，这种操作还可以提高业务场景的灵活度，因为在侧链上我们可以为不同的场景制定不同的区块同步时间，以方便业务逻辑的及时执行。

DMNetwork

数据存储和加密

面向深度挖掘和大数据处理的分布式存储：HDFS

DMChain采用最先进的分布式存储系统来存储其广告和交易数据。我们了解客户数据的价值，因此我们将它们以多次备份的方式存储在Hadoop分布式存储系统中。这意味着即使在数据中心发生意外的情况下，如大规模服务器故障甚至数据中心停电，数据也是安全的。经过慎重考虑，我们选择采用HDFS [5]。它不仅可以使DMChain安全地存储客户的数据，而且还允许DMChain高效地执行大数据分析任务，例如机器学习和数据挖掘。从而DMChain能够利用数据中学到的启发更好地为客户服务。

HDFS目前是面向深度挖掘和大数据处理的基础架构先进存储技术。具体来说，HDFS是Apache Software Foundation项目，它是Apache Hadoop项目的子项目。 Hadoop非常适合存储大量数据（比如TB和PB），并使用HDFS作为其存储系统。 HDFS允许我们连接包含在多台计算机或群集中的节点（通常是虚拟机），并在这些计算机上分发数据文件。然后，我们可以将数据文件作为无缝文件系统进行访问和存储。数据文件的访问以流式处理，这意味着应用程序或命令可以通过MapReduce处理模型直接执行。此外，HDFS具有容错能力，并可提供对大型数据集的高吞吐量访问。因此，HDFS是我们大型数据集的理想分布式存储系统，即广告相关数据。

DMChain

HDFS与其他分布式文件系统有许多相似之处，但有一些差异。一个明显的区别是HDFS的“一次写入多次读取”模型，它减少了并发控制需求，简化了数据聚合，并支持高吞吐量访问。这也是DMChain选择使用HDFS的主要原因，因为广告数据是不可变的，即它们是只读数据记录，需要以高并发性访问。

DMChain实现了HDFS的许多功能。 下面列出了DMChain部署的HDFS中的一些最重要的属性：

1. 通过检测故障并应用快速自动恢复来实现容错
2. 简单可靠的聚合模型
3. 处理逻辑转移到数据，而不是数据转移到处理逻辑以达到最小的数据转移
4. 在多样化硬件和操作系统上的可移植性
5. 可靠的存储和处理大量的数据可扩展性
6. 通过在多个计算机集群上分发数据和处理来节省成本
7. 通过将分布式数据和逻辑并行处理到数据所在的多个节点来提高效率
8. 通过自动维护多个数据副本并在发生故障时自动重新部署处理逻辑来实现可靠性

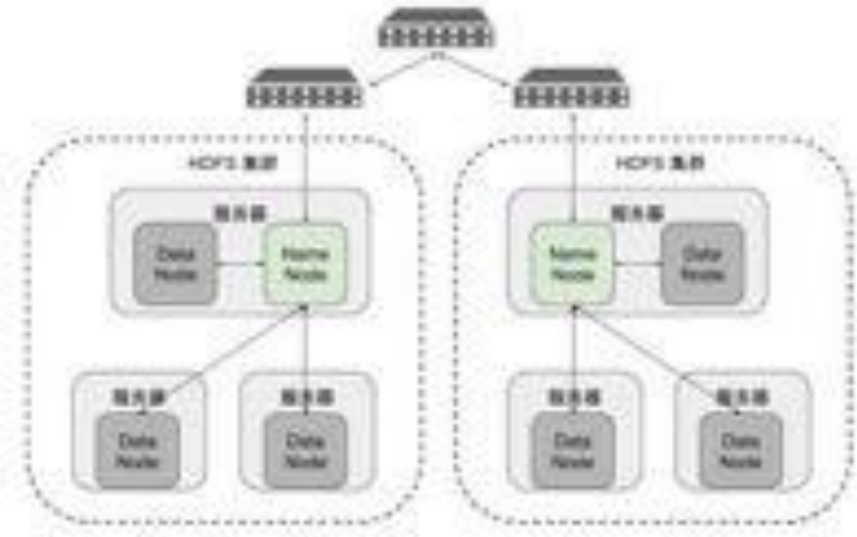

图11. DMChain 多个HDFS集群架构

硬件级零知识证明：SGX™（Software Guard Extensions）

DMChain愿景的一种数据加密方案是，即使在数据处理期间数据也是被严格加密的。众所周知，同态加密能够满足这个愿景，但是这项技术还不成熟，它要么限制了可以对数据集执行的操作类型，要么会导致系统性能的显着下降。因此，我们选择采用更先进的加密技术，即SGX™加密技术 [7]。SGX™硬件加密允许DMChain保护敏感的客户和广告数据，而不会牺牲系统的功能和性能。它使DMChain能够为客户端和广告数据构建最先进，最安全的存储，而且能够支持在加密下的任何类型的数据操作。

具体而言，SGX™代表Intel Software Guard Extensions。顾名思义，它是英特尔系统公司（IA）软件安全性的延伸。这种方法不是识别和隔离平台上的所有恶意软件，相反的，它将合法的软件安全的封装在一个叫做Enclave的区域中，并保护其免受恶意软件的篡改。所有软件，不管是特权或非特权软件都将无法访问Enclave。也就是说，一旦软件和数据在Enclave中，即使操作系统和虚拟机管理程序也不能影响Enclave中的代码和数据。Enclave的安全边界只包含CPU和自身。由SGX™创建的Enclave也可以理解为可信执行环境（TEE）。 SGX中的一个CPU可以并行运行多个Enclave，这是由DMChain存储系统支持的。

采用DMChain SGX技术，系统通过切换CPU的硬件模式进入可信模式，仅使用必要的硬件形成完全隔离的特权模式，加载微型微内核操作系统以支持任务调度，并基于认证用户的身份，完成身份认证。

图12. DMChain使用SGX技术安全的处理加密数据

图12说明了在安全的Enclave中处理用户提交的功能。首先，用户的密钥由DMChain中间件以及Enclave验证。然后，安全区在安全的Enclave环境中解密所请求的数据。数据解密后，Enclave使用用户提交的功能处理数据。最后，处理结果被加密并返回给DMChain客户端，解密后返回给调用程序。

通过使用DMChain SGX加密技术，将Enclave建设为完全隔离的特权模式的具体实施方案如下：

1. 将虚拟机映像加载到磁盘上。

2. 为加密的应用程序代码和数据生成密钥证书。DMChain SGX技术提供更先进的密钥加密方法。其密钥由SGX版本密钥，CPU密钥和DMChain分配给用户。新密钥是在密钥生成算法下生成的。该密钥用于加密要加载的应用程序的代码和数据。

3. 首先将应用程序的代码和数据加载到SGX装载机中。SGX装载机准备将其装载到Enclave中。

4. 在DMChain SGX可信模式下动态构建一个Enclave。

5. 要加载的程序和数据首先由密钥证书以EPC（Enclave Page Cache）的形式解密。SGX指令用于证明解密的程序和数据是可信的，并被加载到Enclave中，然后复制每个载入Enclave的EPC内容。

6. 由于使用硬件隔离，Enclave的机密性和完整性得到了进一步保证，确保不同的入Enclave之间不会发生冲突，并且阻止入Enclave之间的相互访问。

7. 启动Enclave初始化程序，继续加载和验证EPC，生成Enclave凭证，加密凭证并将它们作为Enclave徽标存储在Enclave的TCS（线程控制结构）中以恢复并验证其身份。

8. SGX隔离完成，硬件隔离的Enclave中的镜像程序开始执行，基于SGX技术的硬件隔离完成。

为了访问SGX Enclave，DMChain SGX认证算法首先确定Enclave模式是否被激活，然后确定访问请求是否来自Enclave。如果请求是来自Enclave，则验证算法继续判断，如果不是，则返回访问失败。根据生成Enclave之前的凭证，它们用于验证访问请求是否源自相同的Enclave。如果是，则授予访问权限。否则，遍历Enclave的身份凭证记录表，替换下一个Enclave凭证以匹配，直到测试所有Enclaves凭证。如果匹配失败，DMChain SGX认证算法返回访问失败。

网络层级及架构

随着区块链技术的发展和越来越多的普通用户开始使用区块链技术，区块链数据呈指数级增长态势。同时，由于这些存储在区块链上的数据需要被不同节点频繁读取和同步，因此区块链技术不能依赖于同构的网络拓扑结构的同时支持高吞吐量的网络数据传输。这意味着区块链的每个节点不能为网络中的所有数据做中继传输。为了解决这个难题，DMChain使用**递归互联网架构（Recursive InterNetwork Architecture，RINA）[8]。**

递归互联网架构是现行主流协议栈TCP/IP的替代架构，此架构在设计层面可以允许异构网络节点加入，并显著提高网络数据传输吞吐量，同时保障数据传输的安全和隐私。递归互联网架构与现有网络架构最根本的区别在于RINA架构中所有网络节点都是进程间通信（Inter-Process Communication，IPC）[9] 的参与者。而在IPC中不同的网络层级的通信会被限定在特定的域及规模，所以RINA网络中仅有一个递归协议的集合，而非不同的或专有的通信协议实现。

递归互联网架构整体框架如下图所示。其中分布式应用进程（Distributed Application Process，DAP)是在信息处理系统中处理特定任务的计算机程序，包含一个或多个应用实体以及关联在DAP上的计算资源，如处理器、存储空间及IPC。而IPC进程（IPCP）是RINA网络的核心部分，它也是分布式IPC设备（DIF）的组成部分，负责在本地实现和支持管理IPC进程的工作。

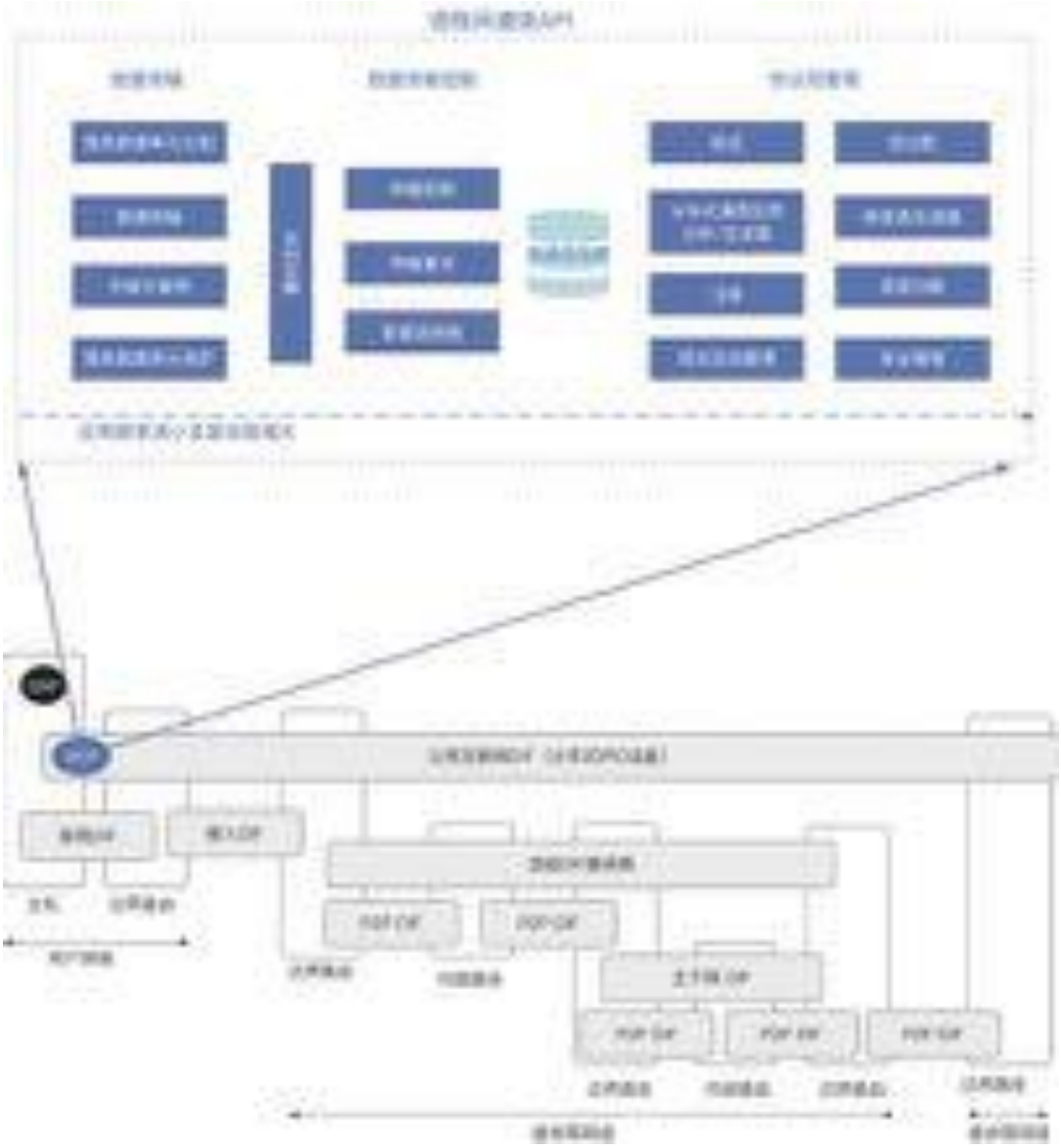

图13. 网络层级及架构

递归互联网架构中的DIF是一些DAP的集合，负责与IPC任务协调与合作。DIF主要向IPC服务提供一套API接口用来与参与某一应用的同级节点交换信息。DIF根据其使用范围和处理能力的区别可被分为多种类型，包括家用DIF，接入节点DIF，P2P DIF，主干网DIF及公用互联网DIF。这些DIF可以实现高性能、高可靠性、高安全性的网络数据传输，同时支持DMChain上的数据快速同步及读写等功能。

可验证安全的权益证明共识算法 — Ouroboros

权益证明算法相比工作量证明算法更为快速高效并能显著降低能源消耗成本，极大提高区块链的性能。同时，DMChain使用的PoS算法为乌洛波罗斯（Ouroboros），它能提供更安全的共识达成机制。在传统工作量证明算法中，矿工会被要求将大量计算资源投入到区块打包的领导者选举过程，而此过程是随机生成的，矿工的计算资源越多则越可能被系统选中进行区块的打包并获得相关的奖励。而在权益证明系统中，区块打包的任务同样是随机选出的，但是系统并不去评估矿工所拥有的计算资源，而系统中用户持有的股份越多则越有可能被选择作为打包者。

权益证明机制在提供更高的区块链每秒交易处理量的同时可以保证投票的安全性。 乌洛波罗斯（Ouroboros）使用了严格的数学证明 [10] 来保障投票的公证公平和安全。其中，乌洛波罗斯（Ouroboros）可以有效避免现有的多种针对区块链的攻击，包括：

1. 多重消费攻击：攻击者利用分布式系统中区块链交易数据不能实时同步的弱点试图对其所拥有的资产进行多次转移。在乌洛波罗斯（Ouroboros）这种类型的攻击不可能成功，因为只要系统中的交易数据是被诚实的参与者确认过的就不再能被修改，而且这些数据会被及时的同步给其它参与者节点上。这样攻击者就不可能将已经被整个系统确认过的信息判为无效。

2. 交易拒绝攻击：在这种攻击中，攻击者试图将某一笔正在被验证的交易拒绝，以破坏他人的交易。这类攻击在乌洛波罗斯（Ouroboros）中也不可能成功，因为乌洛波罗斯（Ouroboros）的在线性质保证了只要有足够多的节点确认某一笔交易，这笔交易就会被确认。

3. 逆同步交易信息式攻击：在这类攻击中，攻击者有意或者无意将区块链信息不与网络中的其它节点进行同步，试图进行离线的交易篡改。乌洛波罗斯

（Ouroboros）不会允许此类攻击的存在，因为所有的交易信息都是被打上严格的时间戳，攻击者不同步最新的区块链信息意味着他的区块信息中包含不正确的时间戳，导致其它网络参与者将其否决。只要少于50%的网络节点是正确同步的，则这类攻击就是不可实现的。

4. 51%攻击：当攻击者拥有区块链51%或者更高的股份时就可以随意篡改数据。首先，在乌洛波罗斯（Ouroboros）中股份的分配是一个严格控制的过程，通常所有参与者的股份分布会非常均匀，这样就能从源头杜绝这个问题。另外，就算某些攻击者成功获取了超过一半的股份，其它参与者也可以很迅速的转移到另一个分叉，从而使得攻击者所获得的股份失去任何意义。

5. 自私挖矿攻击：在这种攻击中，攻击者将打包的某些区块保留一段时间，并等到适当的时候发布出去试图将诚实的节点所打包的区块从主链上消除。在传统比特币的奖励机制中，这种行为可以使得攻击者有更高的奖励。但是在乌洛波罗斯（Ouroboros）中这些行为会被中立化。这就意味着攻击者并不能从此类行为中获取任何额外的奖励，从而鼓励参与节点及时将正确打包的区块发布至主链。

显然，乌洛波罗斯（Ouroboros）的安全性不仅仅是这些，由于其安全性能被从数学角度进行证明，因此我们选择它作为DMChain的共识算法。这个共识算法可以让我们将系统的运营成本降到最低，同时支持并行增长和同时保留多条区块链的能力。这样DMChain就能有极高的安全性、极高的可靠性和极大的灵活性。

算法数学基础

我们首先提供我们协议设计方法的总体概述。协议 [3] 的细节取决于如下几个参数：(i) k 是某个消息为了成为分类账的不可变历史的一部分时最少得到的确认数量，(ii) ε 是诚实的利益相关者对比破坏利益者的有利值；(iii) D 是施加在对手身上的破坏延迟，即当敌手在执行期间传递破坏消息时，诚实的利益相关

者将在时间 D 段后被破坏；（iv）L 是系统的寿命，以时间段计量；（v）R 是一个时隙的长度，以时间段为单位。我们提出了四个阶段来描述协议，逐步改进它可以承受的对抗模型。在所有阶段，“理想功能” $F_{LS}^{D,F}$ 可供参与者使用。该功能捕获可用于各方的资源作为协议安全操作的前提条件（例如，初始模块将由 $F_{LS}^{D,F}$ 指定）。

$$F_{LS}^{D,F} = f(D, F, L, S)$$

阶段1：静态利益，$D = L$

在第一阶段，信任假设是静态的，并与最初的利益相关者保持一致。有一个初始的利益分配，它被硬编码到包含利益相关者公钥的初始区块 $\{(vk_i, s_i)\}_{i=1}^{n}$。基于我们对环境的限制，带有优势 ε 的诚实的多数利益相关者被假设在这些初始利益相关者中，环境最初将允许一些利益相关者的破坏行为，其相关利益可以表示为 $\frac{1-\varepsilon}{2}$，其中 $\varepsilon > 0$。运行环境允许群体破坏行为，向对手提供这种 $(Corrupt, U)$ 形式的Token。值得注意的是，由于第一阶段包含破坏的延迟，任何进一步的破坏行为都将与最初没有利害关系的利益相关者发生对抗，因此这种破坏模式类似于“静态破坏”。$F_{LS}^{D,F}$ 随后将对样本进行取样，以股权”利益相关者抽样加权”，并以这种方式选择 m 个密钥的子集 $vk_{i1}, \ldots, vk_{im}$ 来组成一个委员会，在m中拥有绝对多数的可能性（这是因为破坏方只拥有 $\frac{1-\varepsilon}{2}$ 的相对股权。在这个情况下m将会和 ε^{-2} 是线性依赖关系）。更详细地说，委员会将会隐含的通过以与其股权成比例的方式在每个时隙L被任命到一个利益相关者。随后，利益相关者将按照时隙分配确定的时间表发布区块。最长的连锁规则将被应用，攻击者可以分解诚实方的区块链视图。尽管如此，我们将用马尔可夫链论证来证明在n个时隙序列上叉可以维持的概率至少以 $\sqrt{n}$ 指数级下降。

定理1：正确的利益相关者在算法中是大多数，这个性质是通过以下公式满足的：

$$N_{malicious} = \frac{1-\varepsilon}{2} * N \preccurlyeq \frac{1}{2} * N, where\ \varepsilon > 0$$

阶段2：具有信标的动态状态，每个时隙有 R 个时间段，其中 $D = R \ll L$

延长上述协议寿命的中心思想是考虑多次调用它的顺序组成。这里我们详细说

明这样做的一种方式，假设信任灯塔定期发出一致的随机字符串。更具体地说，灯塔，在时隙 $\{j \cdot R + 1, \ldots, (j+1) \cdot R\}$，揭示领导选举函数的第j个随机串的种子。这个算法与静态协议相比的关键区别在于，股权分配可以改变，并且从区块链本身获取。这意味着在属于第j个时隙 $(j \geq 2)$ 的某个时隙 sl 中，所使用的股权分布是在时间戳小于 $j \cdot R - 2k$ 的最近的块中报告的。

关于不断发展的股权分配，交易将通过环境持续产生并在利益相关者之间转移，玩家将在他们维护的基于区块链的分类帐中加入已发布的交易。为了适应正在创建的新账户，$F_{LS}^{D,F}$ 功能可以根据需要创建新的 (vk, sk) 并分配给新的用户 U_i 。具体来说，环境可以创建新的参与者，他们将与 $F_{LS}^{D,F}$ 通过公共/秘密密钥进行交互，从而将其视为维护其钱包私密性的可信组件。值得注意的是，攻击者可以干涉新用户的创建，破坏它，并代替的提供自己的（对手创建的）公钥。和上述阶段一样，环境可以请求来自利益相关方的账户之间的交易，也可以代表破坏的账户与对手合作产生交易。回想一下，我们的假设是．在任何时候，从任何诚实的角度来看，利益相关者中诚实的相关者总是以 ε 的优势满足多数。（请注意，不同的诚实参与者可能会在某个时段感知不同的利益相关者分布）。此外，股份可以在一定数量的时隙内移动最多统计距离。此处的统计距离将会考虑到基本分布是由加权采样器以及它如何在指定的时间间隔内变化来测量。安全性证明可以被看作是通过静态利益协议的证明提供的基本情况中的时期 $\lceil \frac{L}{R} \rceil$ 的数量的归纳。最后我们认为，在这种情况下，一个 $\frac{1-\varepsilon}{2} - \sigma$ 限制足以保证一次运行中的安全性（并且选择委员会的规模 m 足以克服大小为 $ln(\frac{L}{R})$ 的附加项，其中系统包括了多个这样连续的时期）。破坏延迟保持在 $D = R$ ，它可以任意选择小于 L 的值，从而使对手能够执行自适应破坏，只要这不是即时的。

阶段3：没有信标的动态状态，每个时隙有 R 个时间段，$R = \Theta(K)$，延迟 $D \in (R, 2R) \ll L$

在第三阶段，我们通过引入一个安全的多方协议和“保证的输出传递”来消除对信标的依赖。通过这种方式，我们可以获得阶段2设计中描述的协议的长效性，但只能在阶段1设计的假设下进行，即只有初始随机串和大多数初始利益相关者

的分布。其核心思想如下：由于我们保证选举出来的利益相关者中的真正的多数将以很高的概率保持，我们可以进一步使用这个选举出来的集合作为参与者来参与安全多方计算（MPC）协议的实例。这将要求选择足够的时隙长度，以便它可以适应MPC协议的运行。从安全的角度来看，与前一个案例的主要区别在于，信标的输出在真正的参与方知道之前就会被破坏方知道。尽管如此，我们仍然会证明诚实的用户团体将在短时间内不可避免地学习到它。为了说明攻击者得到这个事实（它可以通过执行自适应损坏来利用这个事实），我们增加了等待时间的合适值，从 R 到在 $(R, 2R)$ 中取得，能够阻止这个优势并且取决于安全的MPC设计。从加密设计的角度来看，这一阶段的特点是使用分类帐本身来模拟支持MPC协议的可靠广播。

阶段4：输入背书人，利益相关方代表，匿名沟通。

在我们设计的最后阶段，我们为运行该协议的实体增加了两个新角色的协议，并考虑匿名通信的好处。在区块包含之前，输入支持者创建第二层交易支持。这种机制使协议能够承受诸如自私挖掘之类的偏差，并且使我们能够证明，在合理假设关于运行协议的成本的情况下，诚实行为是一种近似的纳什均衡。请注意，输入批注者按照时隙领导者的相同方式分配给时隙，并且只有符合条件的输入代言人批准，才能接受包含在块中的输入。其次，代表团的特点是允许利益相关者将委员会的参与转交给选定的代表，承担利益相关方在运行议定书方面的责任（包括参与MPC和发布区块）。代表团自然会产生“利益集合”，它可以像比特币中的矿池一样行事。最后，我们观察到，通过包含匿名通信层，我们可以消除在我们的分析中施加的破坏延迟要求。这是以增加诚实方的在线时间要求为代价的。

DMChain中间件

DMChain dSSP（分散式SSP）

分散式SSP是网络节点软件。 ÐApp将使用该软件为广告和用户交互进行实时广告投标。dSSP可以是应用程序的一部分，可以执行客户端功能并可以在不同

的网络节点上启动。不同节点通过dRTB协议交互，dRTB协议规定，各方都使用分散的安全措施来实时协商和分配利润。如果发生争议，dSSP可以将所有交易数据存储在dRTB事件日志存储中供发布商或审计提供商进行后续分析。

DMChain dDSP（分散式DSP）

分散式DSP是通过dRTB协议进行投标的软件。 DMChain提供自己的dDSP实现，并提供自助服务接口模块，可让广告主管理广告投放活动。DMChain dDSP将协助广告客户适应DMChain生态系统。预计传统的DSP和交易平台将使用dRTB协议，其先进的定位和优化算法，将成为广告主更有效的切入点。

DMChain dDSP 网关

DMChain创建dDSP网关，使传统的DSP通过简单的集成过程连接到DMChain生态系统，并且可以将DMChain资源与其传统广告业务并行使用。为了开始投标，传统的DSP需要购买DM币以获得流动性，并在DMChain注册为dDSP。

DMChain dSSP网关

DMChain创建dSSP网关，使传统的SSP和广告网络能够通过简单的集成流程连接到DMChain生态系统。传统的SSP将根据其流量获得DM币，并在需要时将其转换为其他货币。

DMChain 审计者/审计节点

DMChain生态系统的一个关键组成部分，用于在dRTB协议中实现防欺诈功能。为了实现前所未有的透明度和安全性，DMChain生态系统将提供特殊类型的市场参与者–审计员。DMChain将发布审计师的基本开源实现。每个拥有足够的网络资源来评估欺诈和其他异常流量的DMChain参与者都有资格成为审核

员。这些参与者需要在DMChain中存储安全存款并注册为审计员。在任何谈判中，签署dSSP和dDSP都可以使用任何注册审计员或要求多个审计员来审查dRTB交易流程。这些审计员将担任第三方仲裁员，以决定是否调整用户、发布者，dSSP和dDSP之间的交易。作为分析过程的一部分，审核员可以提供以下判别：

- 用户是正常操作的概率是多少?
- 用户伪造数据的概率是多少?
- 发布商违反广告主的品牌安全政策的概率是多少?
- 广告客户违反发布商的广告政策的概率是多少?
- 广告客户违反用户广告政策的概率是多少?

通常情况下，交易将在短暂暂停后继续进行，以允许审计员收集有关参与者的行为数据，以实现更准确的判别。所有交易流量的汇总数据将由有关各方签署并作为DMChain在dRTB事件日志存储，并建立声誉机制。灵活的声誉机制将允许所有生态系统参与者在通过dRTB进行交易时对出价进行加权决策。如果参与者表现出不恰当的行为，这些参与者将受到潜在合作伙伴的审查，这可能会导致流量的减少，甚至是出价的减少。通过这种设置，所有参与者都可以获得适当的行为激励，从而保证更高的市场效率。

DMChain dDMP网关

通过提供API来奖励用户共享数据，DMChain为DMP开辟了一个公平透明的市场，收集，引导和作为商品实现DMP，将其处理并呈现给数据消费者，并且使用这些数据产生收入。DMChain将实现一个dDMP网关库，该库使用协议来奖励用户数据分享，dDMP网关库将与传统DMP集成，并简化其在DMChain生态系统中的使用。

DMChain

员。这些参与者需要在DMChain中存储安全存款并注册为审计员。在任何谈判中，签署dSSP和dDSP都可以使用任何注册审计员或要求多个审计员来审查dRTB交易流程。这些审计员将担任第三方仲裁员，以决定是否调整用户、发布者，dSSP和dDSP之间的交易。作为分析过程的一部分，审核员可以提供以下判别：

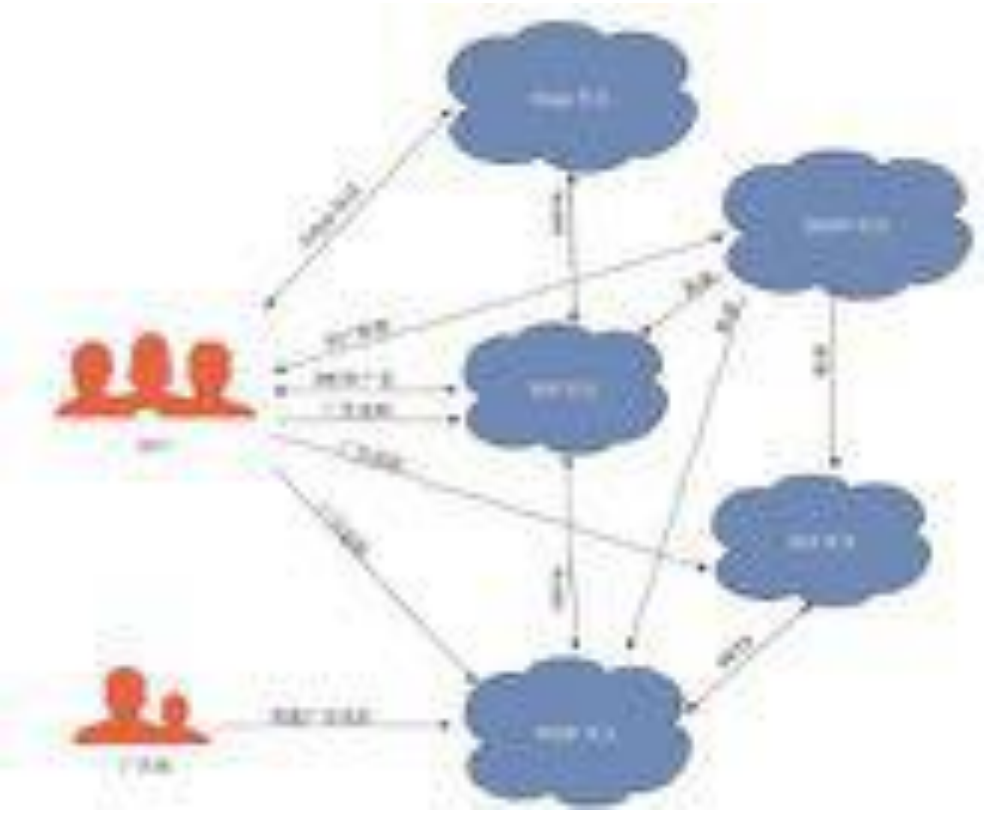

图14. 用户、广告商、DApps和中间件之间的交互

DMChain应用层

DMChain系统包括在DMChain生态系统中建立完整的数字广告所需的所有组件。在前面三层DMChain体系结构的基础上，开发人员将能够构建任何种类的具有集成广告货币化经济效益的应用程序，并在DMChain生态系统中使用。所有与DMChain集成的应用程序将构成DMChain系统的第四层 – 应用层。

SDK和API

DMChain将开源以下SDK以支持开发和应用DMChain生态系统的API。DMChain将发布iOS SDK，Android SDK和JS库，以支持：

- dRTB协议逻辑的封装；
- 用于将广告货币化模型集成到应用程序的API；
- 与DMP共享用户数据的API；
- 用于建立和优化数据共享政策的API，包括数据共享和适当用户奖励的平衡机制；
- 用于设置和调整广告政策的API，包括平衡广告曝光度和广告投放费用。

DMChain生态系统将持续提供软件升级以支持ÐApp中的新广告格式。在第一版中，DMChain将支持简单的横幅广告，随后的版本中，DMChain将支持更多的广告格式，例如视频和原生广告。DApp开发人员可以自由使用自己的广告实现，并在DMChain平台与dRTB协议一起工作。

DApps

DMChain将发布一系列针对DMChain生态系统的应用程序ÐApps：
DMChain用户帐户管理程序。这个应用程序允许用户：

- 注册他们的身份并获得DMChain ID；
- 使用DMChain ID绑定Cookie，以便通过使用dSSP网关连接到DMChain的接收在传统网站和移动应用上通过DMChain显示的广告的付款；
- 配置个性化的广告政策——用户想要看什么广告以及以什么价格购买；

DMChain

- 配置个性化的数据策略——用户愿意与谁共享什么数据，以什么价格购买；
- 显示广告和数据分享的统计数据并获得收益；
- 身份核实后提取收益。

DMChain广告发布商帐户管理程序。此应用程序允许发布商执行以下操作：

- 在发布商注册处注册其身份并获得DMChain ID；
- 为其应用在DMChain生态系统中创建广告；
- 为每个广告设置显示策略 – 发布商准备怎样展示广告以及以什么价格展示；
- 显示广告互动的统计数据，收到的点击数和声誉；

分散式交易所。分散式交易所是DMChain生态系统的理想选择，DMChain团队将开发这个分散式交易所。分散式交易所将允许广告主简单地发布具有明确定义的广告和愿意支付的广告费用，分散式交易所将使用许多会员营销商的力量来实现它们。下面是一些可以构建在DMChain项目上的应用的示例：

- dSSP调解器 – 随着DMChain使用量的增长，发布商可能会看到不同的dSSP解决方案。参与者的优势在于他们允许使用多个dSSP来最大化收入。dSSP调解器可以通过客户端或通过中间网络节点来实现；

- 交易所网络网关 – 一种应用程序，用于汇总来自传统网络的广告并将其发布到分散式交易所。这些网关的所有者可以在DMChain生态系统中得到一定的收益；

- 数据跟踪和分析提供商 – 数据对于有效的广告活动和确保网络的公平性至关重要。使用数据分析来寻求改善更精确的广告投放的解决方案是非常必要的，它将使得广告产生更好的效果。

DMChain

内容审核权益证明/ Content Check Proof of Stake / CPoS

在数字广告系统中大多数的付款交易都是基于点击的（CPM），然而这个奖励机制与广告系统的初衷并不完全一致而导致了各式各样的问题。当广告发布者展示的广告达到一定的数量之后，广告主会付给他一个预先约定好的价格。然而CPM机制是一个非常弱的广告效果评估方法，即广告的展示次数并不代表好的传播效果，而且不同的发布者会有不同的评估标准，导致明显不同的传播效果。

图15. 奖励机制

DMChain

在DMChain中，我们运行用户与广告进行交互，以用户交互的频率和总量来评估广告的实际投放效果。由于区块链的透明性，DMChain可以很大程度减少传统数字广告系统中的欺诈问题。同时，由于用户与广告的交互质量成为广告的投放效果指标，广告主广告的投放效果会更好，进而吸引更多的广告商来DMChain投放广告。

另外，由于这些业务逻辑都是由智能合约自动执行的，这样广告商与分发商的信任不再是一个问题。这样有利于促进广告行业更公平的竞争，逐步形成良性循环从而构建一个生机勃勃的广告生态系统。为了激励普通用户与广告进行交互，用户可以收到部分代币奖励。而普通用户持有代币的行为也可以促进代币生态的良性发展，使得底层区块链权益证明系统中的股权分布更加分散，从而进一步保障底层架构的安全性。另一方面，用户可以自由交易获取的代币，这样可以增加代币的流动性，并吸引更多用户加入DMChain。

DMChain

实施计划

DMChain发展规划（2018 Q1 – 2023 Q1）

2018 Q2	完成基于区块链技术的去中心化数字广告解决方案的设计，并发布白皮书。
2018 Q3	完成DMChain代币ADE的首次数字资产置换。
2018 Q4	搭建DMChain生态，与国内外多家区块链媒体门户及自媒体达成战略合作。
2019 Q1	DMNetwork数字广告网络SDKs发布，引入媒体主参与。
2019 Q3	基于智能合约的DMExchange数字广告交易所上线。
2019 Q4	发布DMID的DApp引入终端用户
2020 Q1	基于PoS的去中心化交易系统。
2020 Q2	包含DMSSP、DMDSP和DMDMP三个模块的DMBaaS区块链即服务平台上线。
2020 Q3	DMChain数字广告链上注册用户达到100万。
2021 Q1	DMChain数字广告链上的交易量超过传统数字广告平台。
2023 Q1	完全去中心化的DMChain数字广告生态系统完成上线。

我们的团队

王青云　　发起人

连续创业者，技术信仰者。在互联网营销领域拥有丰富、专业的实践经验，对企业发展各阶段对市场营销需求具有深刻理解; 2010年，联合创办人人折团购导航平台，获百万级天使投资，并迅速发展成为国内第二大团购导航网站。2013年，联合创办比特币交易网，是中国五大比特币交易所之一，并在日本、澳洲设有分部，获得神州付、亚杰基金等多家投资机构投资; 2015年，创办数字营销SAAS平台DMLei,致力于为中小企业解决营销难的问题，打造智能营销新生态。创业数字营销SAAS平台DMLei,致力于为中小企业解决营销难的问题，打造智能营销新生态。

卢明星　　运营负责人

互联网连续创业者，2008年加入创业公司，独立负责后端系统开发与项目管理，公司于2010年拿到4000万A轮投资; 2012年创办酷拉丁家装020平台，创业初期即获得天使投资，2015年被元洲集团收购并成功退出。

我们的团队

詹小乐　市场负责人

传媒行业连续创业者、2014年度十大策划专家、中国高级商务策划师;曾任照明行业第一媒体《古镇灯饰》、《中国陶瓷》周刊主编、总编;中国家居行业主流媒体《产经评论》出品人、兴邦产业集团报刊中心总经理。

李锋　技术负责人

北京大学计算机硕士毕业(大数据方向) 20年技术研发工作经验，10年技术总监岗位经验;对企业建立数据仓库和数据挖掘以及如何应用数据挖掘支持企业的决策分析有浓厚的兴趣和一定的实践经验;对有关互联网、移动互联网和电子商务的新技术、新概念非常了解。

POLIN AL EKSANDR　系统架构师

5年技术工作经验，覆盖桌面软件、移动软件和基于Web的应用程序。2016年任职consult.ru时与技术团队主导开发基于区块链技术的企业私有链，帮助第三方企业上传不希望被篡改的文档。

我们的团队

唐集荣　项目顾问

S.Capital（一致资本）创始人，资深通讯行业专家，互联网连续创始者，曾任职于世纪海翔投资集团，负责FOF&VC投资；在区块链和数字货币领域有着丰富的股权投资和数字资产投资经验。

孙泽宇　项目顾问

创世资本创始人，库神冷钱包的联合创始人，北京大学金融科技创新实验室区块链顾问委员。

Tabitha Tao　项目顾问

资深营销经理，加拿大西蒙弗雷泽大学研究生院MBA研究生，精通数字营销和品牌管理，擅长制定与执行Facebook、Twitter，Youtube等社交媒体营销战略，拥有超过十年线上&线下市场营销经验。曾任思科中国（Cisco）品牌经理，荣获2004–2009连续5年思科业绩计划(CAP)奖，2009年思科APAC最佳市场执行提名。

投资人

韩大为
DKB创始人
曜为资本创始合伙人

丁浩（融合）
coinbig联合创始人

赵千捷
BTCC高级副总裁

拓拓
加密愿景创始合伙人

张太阳
Coinmarket CEO

张俊宇
浩方创投管理合伙人

投资机构

GENESIS 创世资本

S·Capital 一致资本

TIMESTAMP CAPITAL

Grand Shores

乐东资本 HAPPY EAST CAPITAL

浩方创投 HOFAN CAPITAL

金刚资本

天际资本 ZenithVentures

WEMEET CAPITAL 预鉴资本

投资机构

DMChain

区块链合作媒体


巴比特
资讯
服务于区块链创新者


耳朵财经


核财经


烯财经
ENE FINANCE


btc123.com


Coingogo
币源社区


雷鹿财经
LEILOOK.COM


OKZ

已服务广告客户（部分）


听云
TINGYUN


喂肚肚


融贝网
rongbei.com


蜂巢互联
HONEYCOMB


麦乐购
GOU.com


UCLOUD


起风了

风险提示

证书丢失导致代币损失的风险

参与代币置换的参与者所置换的代币在分配给参与者之前很可能被关联至一个DMChain的账号，进入DMChain主链平台账号的唯一方式就是参与者选择的相关登录凭证，遗失这些凭证将导致代币的遗失。最好的安全储存登录凭证的方式是参与者将代币分开到另一个或多个地方安全储存，且最好不要暴露在工作的地方。

以太坊核心协议相关的风险

在Cardano智能合约上线前，代币和DMChain应用程序基于以太坊的协议开发，因此任何以太坊核心协议发生的故障，不可预期的功能问题或遭受攻击都有可能导致代币或DMChain应用以难以预料的方式停止工作或功能缺失。此外，以太坊协议中账号的价值也有可能跟代币相同的方式或其他方式出现价值上升或下降。
关于以太坊协议的其它信息： http://www.ethereum.org。

购买者凭证相关的风险

任何第三方获得购买者的登录凭证或私钥，即有可能直接控制购买者的代币，为了最小化该项风险，购买者必须保护其电子设备以防未认证的访问请求通过并访问设备内容。

风险提示

司法监管相关的风险

区块链技术已经成为世界上各个主要国家的监管主要对象，如果监管主体插手或施加影响，则DMChain应用或代币可能受到其影响，例如法令限制使用、销售，电子代币诸如BTC、ETH、ADA、ADE皆有可能受到限制，阻碍甚至直接终止DMChain平台应用的发展。

应用缺少关注度的风险

DMChain社区应用存在没有被大量个人或组织使用的可能性，这意味着公众没有足够的兴趣去开发和发展这些相关分布式应用，这样一种缺少兴趣的现象可能对DMChain社区应用造成负面影响。

应用或产品达不到自身或购买者预期的风险

DMChain平台应用当前正处于开发阶段，在发布正式版之前可能会进行比较大的改动，任何DMChain社区自身或参与者对DMChain社区应用或代币的功能或形式（包括参与者的行为)的期望或想象均有可能达不到预期，任何错误的分析、设计的改变等均有可能导致这种情况的发生。

黑客或盗窃的风险

黑客或其它组织或国家均有以任何方法试图打断DMChain应用或代币功能的可能性，包括服务攻击，Sybil 攻击，恶意软件攻击或一致性攻击等。

漏洞风险或密码学发展的风险

密码学的飞速发展或者科技的发展诸如量子计算机的发展，或将破解的风险带给加密代币和DMChain社区，这可能导致代币的丢失。

缺少维护或使用的风险

首先代币不应该被当做一种投资，虽然代币在一定的时间后可能会有一定的价值，但如果DMChain主链缺少维护或使用的话，这种价值可能会变得非常小。如果这种情况发生，则可能该平台将会没有后续的跟进者或少有跟进者，显然，这对代币是非常不利的。

未保险损失的风险

不像银行账户或其它金融机构的账户，存储在DMChain平台账户或以太坊网络上通常没有保险保障，任何情况下的损失，将不会有任何公开的个体组织为你的损失承保，但诸如 FDIC 或私人保险公司将会为购买者提供保障。

项目解散的风险

存在这样的可能，出于各种原因，包括价格的波动，DMChain应用发展遭遇问题，生意关系的破裂或知识产权索赔等可能的原因，DMChain项目随时都有可能遭遇重大打击或直接解散。

DMChain

应用存在的故障风险

DMChain平台可能因各方面的原因故障，无法正常提供服务，严重时可能导致用户代币的丢失。

无法预料的其它风险

密码学代币是一种全新且未经测试的技术，除了本白皮书内提及的风险外，此外还存在着一些DMChain团队尚未提及或尚未预料到的风险。这些风险也有可能突然出现，或者以多种已经提及的风险的组合的方式出现。

参考文献

[1] Nakamoto S. Bitcoin: A peer-to-peer electronic cash system.
[2] Buterin, V., 2013. Ethereum white paper. GitHub repository.
[3] Kiayias A, Russell A, David B, Oliynykov R. Ouroboros: A provably secure proof-of-stake blockchain protocol. In Annual International Cryptology Conference 2017 Aug 20 (pp. 357-388). Springer, Cham.
[4] Van Deursen, A. and Klint, P., 2002. Domain-specific language design requires feature descriptions. Journal of Computing and Information Technology, 10(1), pp.1-17.
[5] Borthakur, Dhruba. "HDFS architecture guide." Hadoop Apache Project 53 (2008).
[6] Siegel, J. ed., 2000. CORBA 3 fundamentals and programming (Vol. 2). New York, NY, USA:: John Wiley & Sons.
[7] Davenport, Shaun, and Richard Ford. "SGX: the good, the bad and the downright ugly." Virus Bulletin (2014): 14.
[8] Klomp, Jeroen van Leur Jeroen. "Recursive InterNetwork Architecture." (2016).
[9] Lamport, Leslie. "On interprocess communication." Distributed computing 1, no. 2 (1986): 86-101.
[10] Mullin, Lenore MR, and Michael A. Jenkins. "Effective data parallel computation using the Psi calculus." Concurrency: Practice and Experience 8, no. 7 (1996): 499-515.

DMChain

基于区块链的去中心化数字广告平台

白皮书3.0