

2018

广告反欺诈白皮书

腾讯灯塔 / 秒针系统 联合发布

Tencent 腾讯



根据CNNIC统计，截至2018年6月，中国手机网民规模达7.88亿，网民通过手机接入互联网的比例高达98.3%，同比增长3.2%。目前，中国每个手机网民下载使用的手机应用数量平均超过十个。手机应用种类不断增长，用户规模不断上升，使用场景愈加丰富。

以手机为代表的移动端设备已成为品牌和广告主开展营销、与消费者沟通的主要渠道。未来，品牌和广告主在移动广告上投入的预算也将不断加大。但与此同时，由于信息不对称和数据可见性的缺乏，移动广告欺诈问题愈加严重，甚至已经成为一种业务成本。Forrester最新研究报告表明，43%的营销人员表示在过去12月内因广告欺诈所浪费的广告预算有所增长，34%的营销人员称其移动广告预算约有超过一半被移动网站广告欺诈和应用内广告欺诈所浪费。

为净化互联网广告市场、促进行业健康发展，腾讯灯塔、秒针系统和AdMaster于2017年4月携手成立了国内首个广告反欺诈大数据实验室，并于2017年10月联合发布《2017广告反欺诈白皮书》。

基于过去一年移动广告欺诈的新情况和新变化，以及作弊方式和反作弊技术的变迁，腾讯灯塔和秒针系统再度携手，向行业推出《2018广告反欺诈白皮书》，旨在厘清当前国内移动营销市场的广告欺诈情况、攻防技术及对策，以期推动移动广告行业的透明度和规范化发展。

第一章 2018年数字广告行业黑产概述

1.1 行业大盘黑产趋势

黑产的从业人员，既包括广告作弊技术及服务的提供者，也包括广告作弊方案的购买者。在广告投放领域长长的链条上，每一个角色都有可能成为黑产的相关者。黑产的作弊方式详见《2017年广告反欺诈白皮书》。从2018年看，黑产流量总体比例与2017年基本持平，维持在15%左右。

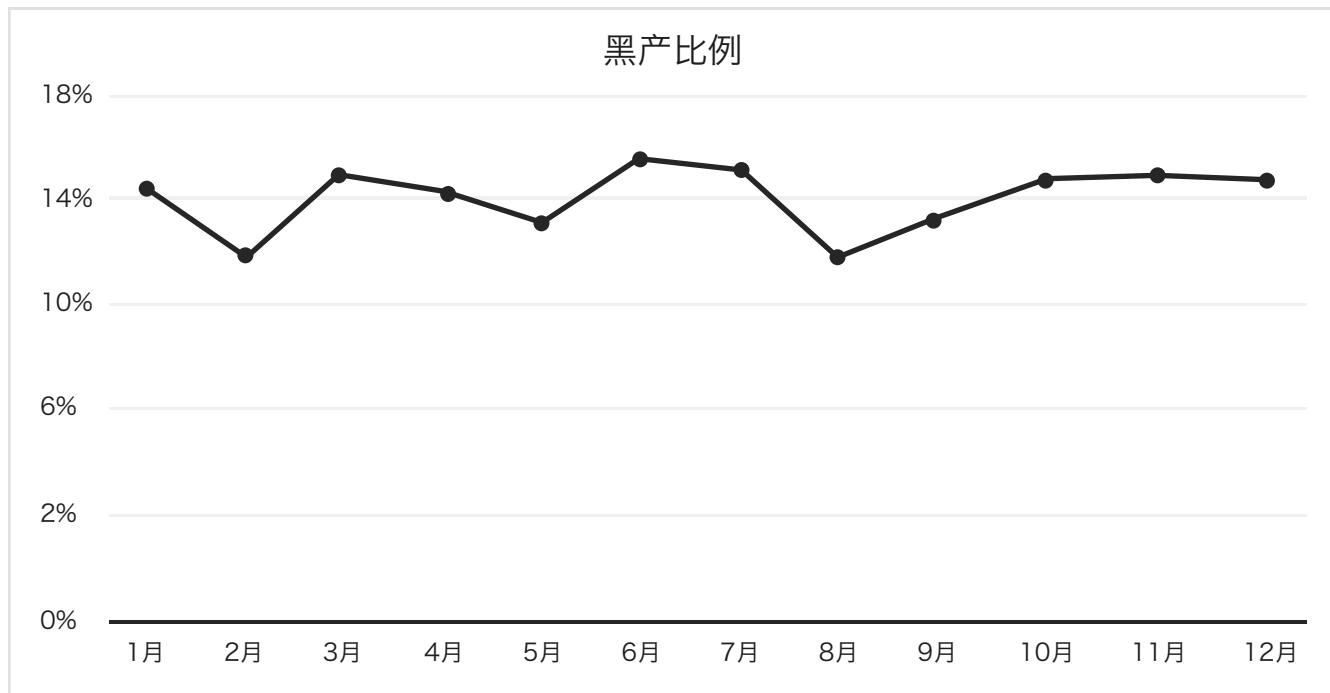


图1 2018年黑产趋势图 / 数据出处：腾讯灯塔、秒针系统广告反欺诈大数据实验室

1.2 黑产新趋势

由于业界正义力量的不断努力，黑产无节制扩张的势头一定程度上得到了遏制，黑产作弊门槛明显提高。2018年，黑产份子中“散户”基本被消灭，集团化趋势愈发明显。集团化的黑产有明确的上下游分工，有完善的技术服务配套保障体系，因此表现出更强大的战斗力。

由于黑产有发达完善的情报、监控体系，和合理的软件架构，一般在运营活动上线当天，就会有相应刷量软件出现。黑产软件架构较为合理，把底层基础服务和上层应用相剥离，只需要修改上层应用部份，就可以实现刷量。如图所示，某业务2018世界杯活动上线四个小时内，就有大量黑产用户开始刷量。

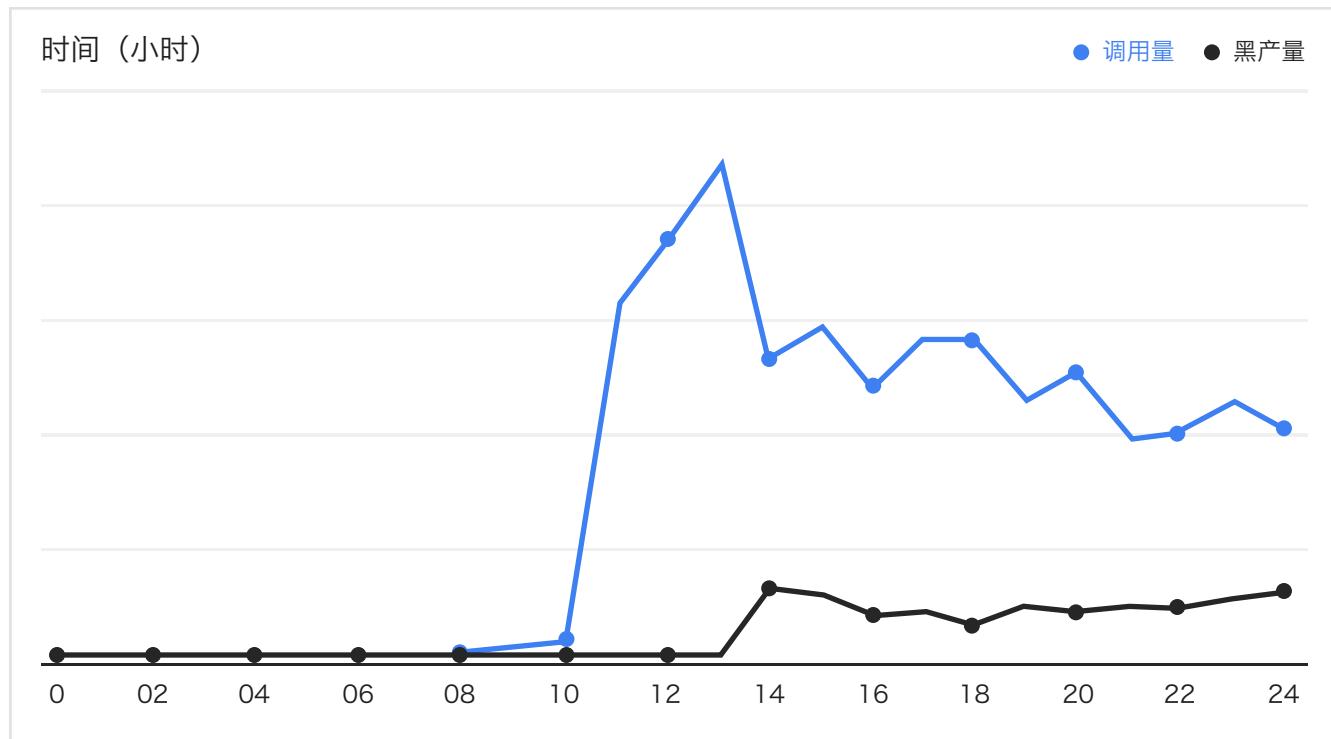


图2 黑產响应速度

黑产刷量软件非常灵活，适用性极强，可对短信接收、线程、带宽、频率、开始时间、打码方式等进行设置。本文随后将对黑灰产产业链从技术角度进行剖析。

第二章 互联网黑灰产业链技术剖析

基于上述对互联网行业的分析，刷粉、刷量、工具软件销售等以及平台相关的牟利方式已经形成了环环相扣的产业链。根据需求，服务一应俱全，从账号商人、工具开发者到代理IP平台、手机卡商、接码平台等，每一层都有成熟的利润获取方式。本章将会从技术手段剖析黑产产业链的构成形式。

黑产盈利直接模式有三种：引流变现、搬运工薅羊毛以及刷量作弊。

- 引流变现：将用户（目标消费群体）引至微信、直播等其它平台，再以微商、诈骗等方式深度变现。
- 搬运工薅羊毛：例如，当平台有补贴等鼓励活动时，采集其它平台优惠/活动信息，修改上传；有时搭配作弊冲击平台的各项指标，骗取现金奖励。
- 刷量作弊：虚假新增、激活用户、刷粉、刷点赞、刷播放量等数据赚取现金。

如下图所示，这三种盈利方式都处于整个产业链的最下游。上游环节的开发者、卡商、代理等高度重合。这说明了黑产上、中游的技术提供商具备平台化的开发和销售能力，能够为花样繁多的作弊手段提供通用化的解决方案。下文将会就黑产产业链的技术形态进行详细说明。

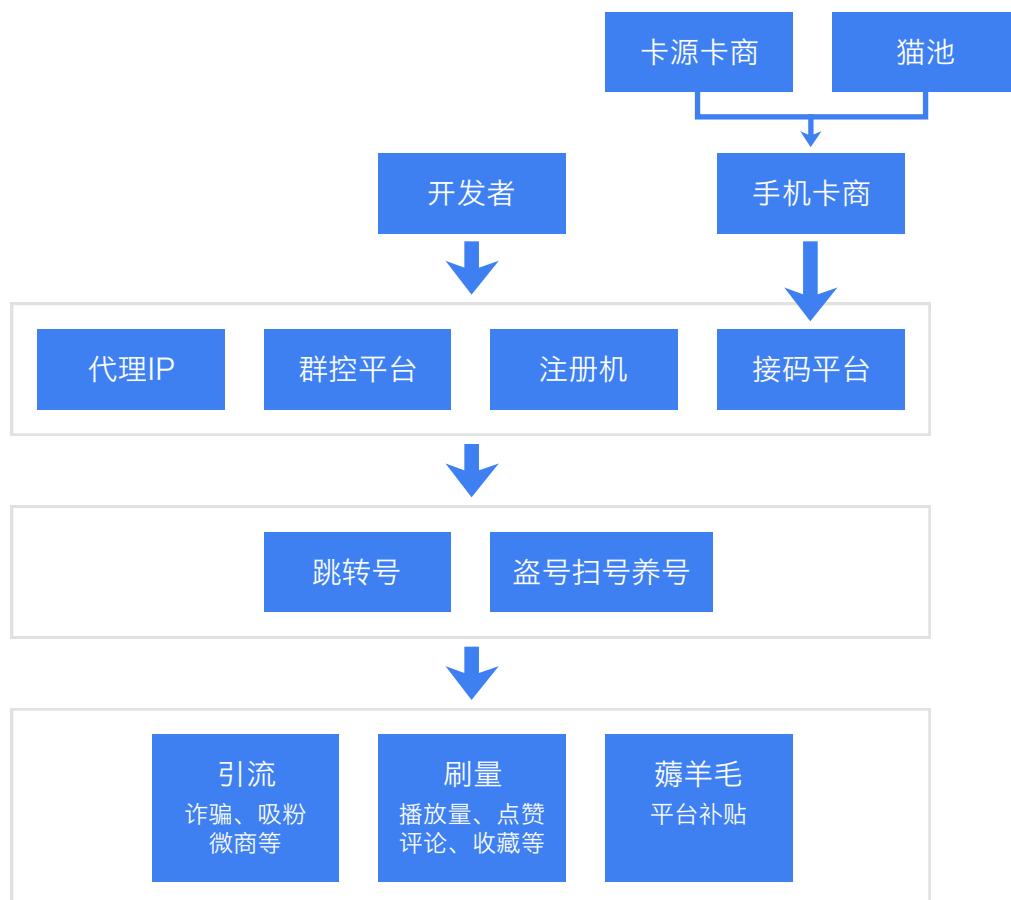


图3 黑产产业链

2.1 手机卡商

手机卡商，能够为接码平台和黑灰产从业者提供大量手机号，用以各种虚假注册、认证业务。这些手机卡被称为黑卡。其上游主要是卡源卡商及猫池为其提供服务。

2.1.1 卡源卡商

1、卡源卡商通过各种渠道（如：开皮包公司、与代理商打通关系等）从运营商或代理商那里办理大量的手机卡，然后加价转卖给下游卡商赚取差价，他们掌握着手机黑卡货源。根据反向追踪调查，卡源主要有：

- 物联网卡：无须实名认证，主要用于工业、交通、物流等领域。物联网卡需要以企业名义办理，卡商以千元左右的价格可轻易购得“营业执照”进行办理，且一张营业执照几乎对办理数量不做限制。
- 实名卡：这种卡多为从网上收集大量身份证信息批量认证得来。
- 海外卡：由于实名制的原因，16年下半年开始，大量缅甸、越南、印尼等东南亚卡开始进入国内手机黑卡产业。这些卡支持GSM网络，国内可直接使用，无需实名认证，基本是0月租，收短信免费，非常切合黑产利益。

2、猫池厂家

猫池厂家负责生产猫池设备，并将设备卖给手机卡商使用。猫池是一种插上手机卡就可以模拟手机进行收发短信、接打电话、上网等功能的设备，在正常行业也有广泛应用，如邮电局、银行、证券商、各类交易所、各类信息呼叫中心等。猫池设备可以实现对多张手机卡的管理。



图4 猫池

2.2 黑IP

黑灰产从业者为了隐藏自己的真实IP，同时也为了绕过甲方的IP风控策略，需要大量的IP资源（比如代理IP）作为跳板，进而发动作弊。用于作弊的IP，即指黑IP。

全球IPv4总数约为43亿，美国拥有30%以上，美国的黑IP数量占比36.39%，遥遥领先其他国家。发达国家的黑IP数量要多于发展中国家，可以简单理解为，发达国家拥有更多的互联网设备，也就拥有更多的IP资源，所以黑IP的数量与互联网设备的数量成正比。

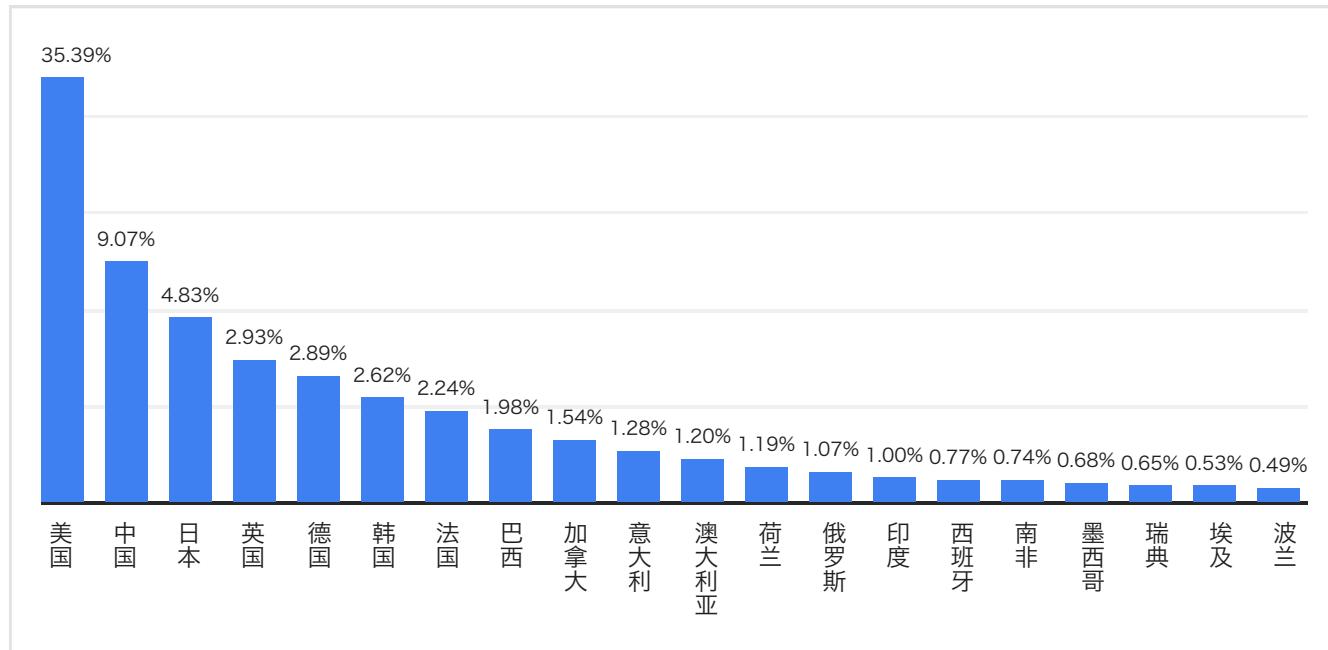


图5 全球黑IP来源国家TOP20

从黑IP来源城市数据看来，上榜的城市都是经济较为发达的城市。

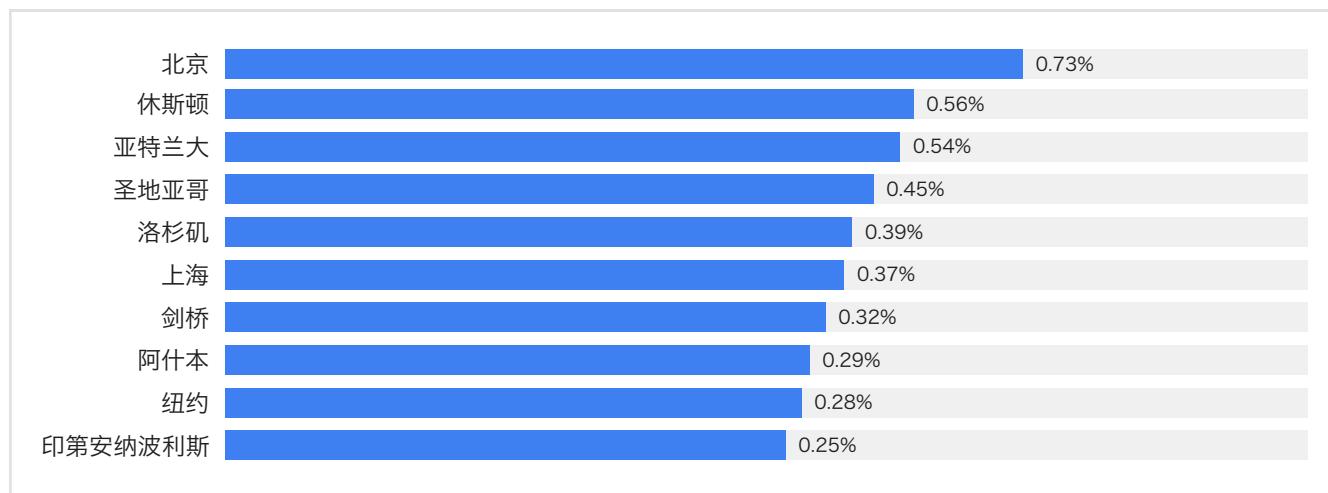


图6 全球黑IP来源城市TOP 10

2.3 接码平台

接码平台负责连接卡商和羊毛党、号商等有手机验证码需求的群体，提供软件支持、业务结算等平台服务，通过业务分成获利。接码平台很多，活跃的有数十家，部份接码平台可以接语音验证码。2016年11月，当时最大的接码平台被警方查处后，很多平台转入地下。平台一般会提供客户端和API接口，接口可以用来对接自动化的工具。根据使用项目的不同（如一些项目只需要识别短信中的验证码，一些却需要发送短信进行验证），平台会合理安排手机卡的使用，用户也可以选择在平台上对接专属卡商，既能节省成本，又能提高自己使用黑卡的质量。



The screenshot shows a web-based SMS verification service interface. At the top, it says "短信验证码服务 SMS Verification Service". Below that, there are several search and filter fields:

- 短信项目:** A dropdown menu with the placeholder "请点击右侧按钮查询项目" (Please click the button on the right to query the project) and a "选择项目" (Select Project) button.
- 运营商:** A dropdown menu with the placeholder "—不限—" (All).
- 归属地:** Two dropdown menus, one with the placeholder "—不限—" and another with "—不限—".
- 排除号码:** A text input field with the placeholder "如: 171|172|174|178".
- 手机号码:** A text input field with the placeholder "请获取手机号..." and three buttons: "获取手机号" (Get Phone Number), "释放手机号" (Release Phone Number), and "加入黑名单" (Add to Blacklist).
- 短信内容:** A large text input area.
- 验证码:** A text input field with the placeholder "验证码" and a checkbox "获取短信后自动释放号码" (Automatically release the number after receiving the SMS).

At the bottom, there are four buttons: "获取短信" (Get SMS), "发送短信" (Send SMS), "获取指定手机号" (Get Specific Phone Number), and "释放全部" (Release All).

图7 接码平台

接码平台上的项目数量和单价，可以侧面体现平台账号批量注册的严重程度以及绕过手机号验证的成本。



The screenshot shows a client application window titled "客户端 V4.9". The interface includes a menu bar with "仅解决互联网个人手机号使用的隐私问题，仅限在法律允许的范围内使用。禁止任何用户使用本站任何功能进行违法操作，否则后果自负" (Only solve the privacy problem of personal mobile phone numbers in the Internet, only within the scope of laws. Any user using any function of this site for illegal operations will bear the legal consequences). Below the menu are several icons: 验证码[收发] (SMS Verification [Send/Receive]), 验证码[收码] (SMS Verification [Receive]), 项目列表 (Project List), 专属对接 (Exclusive Cooperation), 明细统计 (Detailed Statistics), 安全中心 (Security Center), 充值 (Top-up), 设置 (Settings), and 退出 (Exit).

The main area displays a table of projects:

项目ID	项目名称	单价	类型	收藏
1	[海外卡专供]	0.15	收码	无
2	e兼职 [兼职]	0.1	收码	无
3	红包	0.1	收码	无
4	夺宝	0.1	收码	无
5	枫车	0.1	收码	无
6	解封[发短信]	0.5	发码	无
7	app注册	0.1	收码	无

图8 接码平台报价

2.4 群控系统

群控系统的使用是为了避过平台对设备的检测。即采用电脑来控制多部移动设备，如下图为针对iPhone的群控系统，能够让连接的多部手机根据既定脚本批量执行操作。对于账号注册部分，系统集成了过滑动验证、自动获取填写验证码、修改资料等功能。

设备名	设备号	设备别名	网络IP	客户端版本	客户端授权	锁屏状态	充电状态	运行状态	连接状态	脚本到期时...	客户端...
04-8.3	iPhone 5e985f...	iOS8	10.0.0.190	1.3.4	已授权	锁	空	空闲	连接	--	2019-01-01
U25GT-C4...	Android 010b32...	s1231...	10.0.0.170	1.0.1	已授权	锁	空	空闲	连接	--	2017-12-31
2013023	Android 2d7fbf4...	红米	10.0.0.41	1.0.1	已授权	锁	充	空闲	连接	--	2017-12-31
1107	Android 55f47c...	oppo 1...	10.0.0.242	1.0.1	已授权	锁	充	空闲	连接	--	2017-12-31
iPhone010	iPhone 317ef5...	iOS8.2	10.0.0.108	1.3.4	已授权	锁	充	空闲	连接	--	2018-01-01
iPhone5S	iPhone 9d0057...	ios10	10.0.0.228	1.3.4	已授权	锁	充	空闲	连接	--	2019-01-01

图9 群控系统

每台设备会存在注册账号数量的限制，这时会结合改机软件来解决。改机软件通过劫持系统函数，修改UDID、IMEI、SSID、定位等设备信息的，使平台检测认为是新的手机。

上述平台结合了一键新机工具，该工具除了修改设备信息，还提供一键新机、多开、全息备份等功能。只对勾选的app更新设备参数，能够导出参数备份信息，为跨机共享和恢复某账号设备环境提供便利。

使用群控系统时，每部手机都会安装既定的Lua脚本去执行触摸，滑动，输入文本等操作，使用者可以根据不同目的找开发人定制专门的脚本。群控系统、脚本和改机工具结合使用，再接入接码平台和代理IP，就可以高效的产出质量过硬的号码。这种方式完全模仿真实用户，较难分辨。厂商可以从“虚假号码”、黑IP、用户行为及进入app后的操作顺序等角度着手判断。

2.5 注册机

注册机多是自动化批量注册的工具，多是采用易语言进行开发，在Windows下运行，技术手法有两种：

- 模拟操作类：通过控件操作浏览器元素实现，真实加载注册页面，模拟用户操作。
- 协议破解类：通过HTTPS协议实现，破解注册接口协议，直接带参数调用注册接口实现注册。

手机号资源自然是接码平台获取，IP资源使用ADSL拨号（使用VPS挂机操作等），这背后也有一条完整的产业链支撑。大多注册机的速度可达到几十秒注册一个账号，为下游的各个细分产业提供大量的小号。

有些平台的策略会对这类账号造成影响，即有些注册机出来的号码，几天内会失效，但仍可以对接“直接用量怼的项目”，一般会采用预定方式售卖账号，随买随用。



图10 注册机

2.6 跳转号

除了直登号外，跳转号也是常见的号码。指使用QQ号、微信号、微博号等快捷登录后，激活绑定而转化而成的平台账号。这里使用的账号并非正常账号，而是称为授权号的特殊账号，这种账号在原有平台质量很低，无法进行大部分业务。所以只用作授权其他平台，购买成本仅几分钱。



图11 跳转号

在互联网灰产领域，许多工作室依赖注册和贩卖各种账号生存，这些账号已经成为了具有广泛销量的基础资源，再流入各个细分产业链。小号虽小，却要在风控战场上引起大的重视。

2.7 盗号、扫号和养号

老号指有一定注册时间、自身带有权重的号码，有的还带有一定的粉丝与作品。这类号码被认为不易封号，在市场上受欢迎。老号和带有一定权限等级的号码，一般是采用这三种方式得到的：

- 盗号：主要方式是钓鱼。如发布二次打包的软件将某些软件打包加入自己需要的功能，当用户使用这些动过手脚的软件时，黑客就会收到他们的账户名、密码。
- 扫号：方法有两种：1、用接码平台的手机号作为用户名，遇到注册过的直接修改密码，这种属于黑吃黑，拿走了别人批量注册的号码。2、使用其他手段获取大量账号名，加上弱密码，去逐一验证，这种账号一般的真实用户，对平台伤害较大。
- 养号：号商注册后模仿真实用户进行一些操作，将号码养老的行为。大多是为了提高账号的权重，以方便之后的黑产项目，对平台伤害较大。

第三章 黑产具体案例

3.1 和黑产在经济层面、技术层面上的双重博弈

黑产团队的行为动作都和经济利益息息相关。黑产往往会选择成本最低、阻力最小的方式切入，碰到阻力时，就会升级为成本更高的方式。



图12 黑产攻防对抗演化

当业务的产品逻辑出现漏洞时，黑产往往会倾向于优先利用产品逻辑漏洞得利。这种方式成本最小，甚至法理上也占优。如，业务如果没有限定一台手机一个账号只能参加一次抽奖活动，黑产可能会利用这一漏洞，反复在一台手机上用多个账号登录。不需要基本的技术、硬件门槛，这种方式对于黑产而言成本最低。由于有一定的技术门槛，而又不需要真实设备的投入，模拟器的报价往往高于利用业务漏洞，而低于真机假用户。由于有实际手机的占有成本，真机假用户的成本会高于模拟器。作弊成本最高的方式是人肉作弊。据腾讯灯塔情报部门分析可知，当个人获利小于3元时，人肉众包的方式很难持续下去。（模拟器、真机假用户的定义可见《2017年广告反欺诈白皮书》）

下面以某产品在某次运营活动当中所经历的攻防对抗来对黑产活动进行分析。

如图13所示，在本例中，由于产品逻辑没有明显漏洞，黑产直接跳过第一步，进入模拟器的形式。灯塔反作弊模式相应启动，对模拟器作弊形为进行了打击。

在模拟器的作弊形式受到打击之后，黑产一边向该业务客服发起恶意投诉，试图通过大量投诉的方式迫使该业务放弃打击；一边将作弊方式转移到成本更高的真机假用户，试图躲避打击。真机假用户同样是在腾讯灯塔的打击范围内，黑产份子没有得逞。同时，腾讯灯塔利用大数据对投诉进行画像分析，发现大量投诉都源自于黑产团伙的恶意投诉。

黑产份子没有死心，仍然一边恶意投诉，一边试图用人肉的方式进行作弊。腾讯灯塔同样利用多业务交叉分析、画像分析，准确判断出恶意份子。由于人肉的方式成本过高，黑产份子受到打击后，发现没有太多的利益可图，就自行退却了。

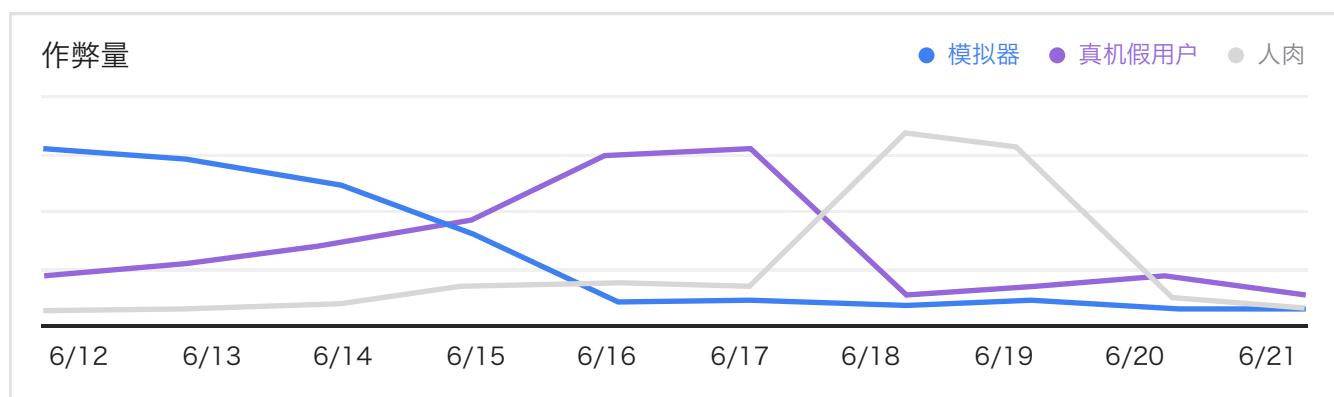


图13 黑产演化实例

3.2 偷天换日，劣质流量替换优质流量

某日用消费品广告主投放在A媒体上的视频贴片广告代码，在B媒体的新闻页面后台进行刷量。经排查发现，B媒体后台添加了A媒体的贴片广告代码。当用户打开B媒体页面时，就后触发多条A媒体视频贴片播放代码，但不会出现视频贴片播放。通过这样的形式，黑产用劣质流量替换了优质流量，实现了超额的收益。

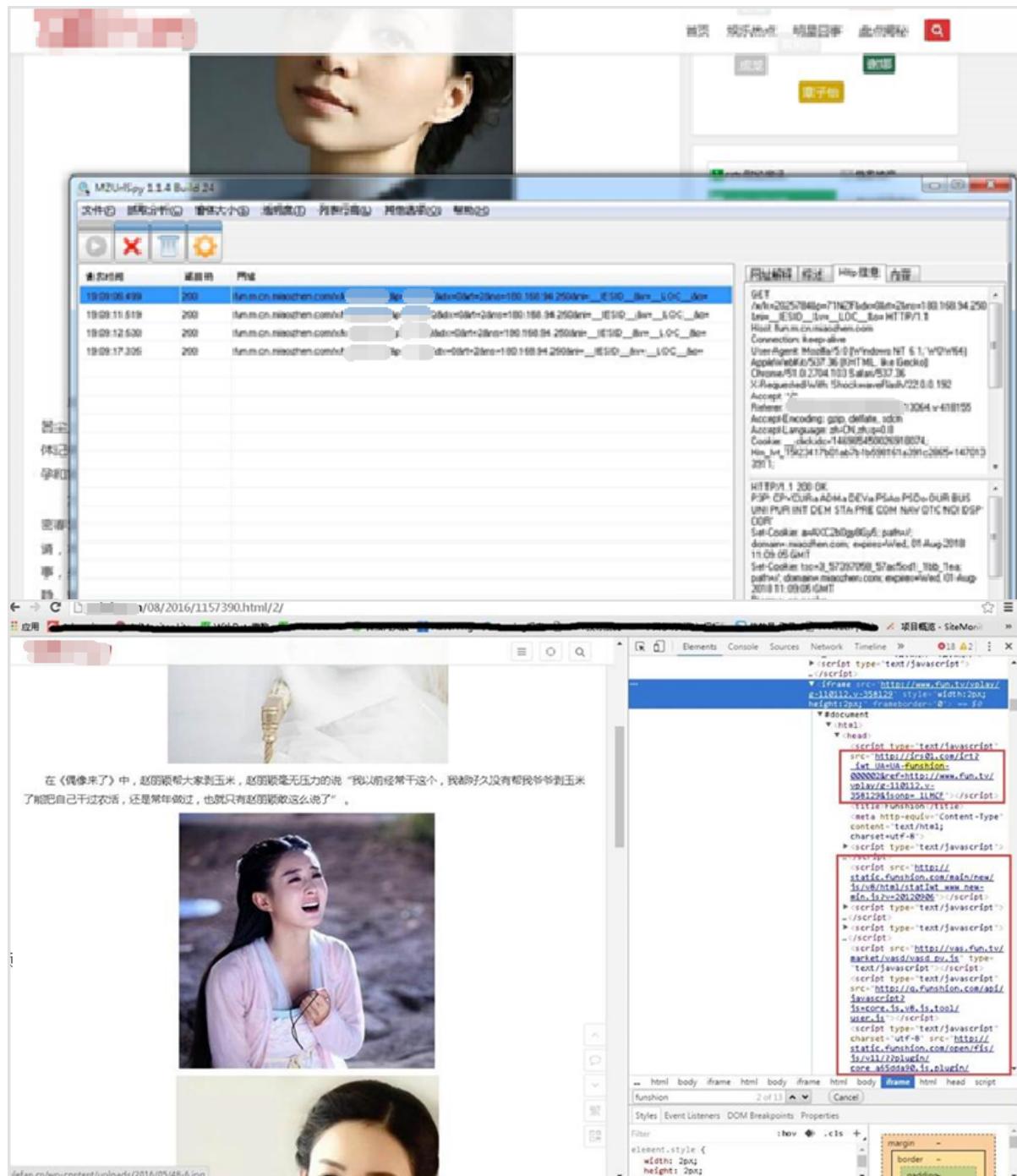


图14 某媒体用劣质流量替换优质流量

第四章 应对方法及安全建议

4.1 灯塔反作弊解决方案

灯塔智能反作弊框架是一套基于终端识别技术与云端交叉验证，利用AI技术建立查模型、杀模型、验模型三管齐下的实时反作弊体系。灯塔智能反作弊引擎拥有灯塔积累10亿终端用户画像，占国内活跃终端的90%以上，占新增终端80%，在此基础建立六大纬度1000+异常特征图谱，积累了亿级山寨机和黑IMEI库，同时结合独有终端防伪技术和业界首创的查、杀、验技术架构，最大限度提升覆盖率、及时性、准确性，有效提高反作弊防范强度和识别精度。



图15 灯塔反作弊解决方案

创新性技术探索

4.1.1 提出独有终端指纹识别方案

1、不同于市场上单一产品终端身份生成方案，终端指纹技术基于腾讯移动领域积累多年的产品大数据，100+头部App数据，以及涵盖社交、游戏付费、垂直领域的业务数据交叉验证，有效解决反作弊的冷启动问题。

2、与业界仅依赖终端应用层信息相比，灯塔智能反作弊的终端指纹，深度覆盖了硬件层、系统核心和系统调用库层、应用框架层3个层面，配合云端离线分析、终端实时身份请求系统，保持终端指纹的高度一致性；

3、结合文件系统识别、指令逃逸检测、内存反馈式检测和系统关键函数字节码检测等技术，终端指纹识别方案有效覆盖模拟器、伪造/篡改设备信息、系统劫持以及虚假激活等作弊场景的篡改用户身份的作弊行为。

4.1.2 业内首创的查杀验技术架构

与业界常规的基于规则的反作弊方案不同，灯塔反作弊提供查-杀-验一体的综合解决方案，能够从作弊发现、作弊稽核/取证以及作弊验证三个环节实施全程监控，并且查-杀-验模型之间的交叉验证形成新作弊场景探测与学习，完成作弊强特征发现与利用以及打击效果验证之间的闭环。

1、查模型：作为灯塔反作弊解决方案的第一层保障机制，查模型涵盖内核/网络层、系统层、应用层以及用户行为层4个层次的异常检测，能够快速全方位地捕捉到用户的异常情况。

2、杀模型：作为灯塔反作弊解决方案的核心环节，杀模型基于规则模型和多项专利反作弊算法模型为业务提供作弊识别和作弊举证服务，输出按恶意等级区分的用户粒度识别结果。同时，杀模型输出高质量的用户标注数据，为实时反作弊系统与离线反作弊的融合提供基础。此外，查模型和杀模型之间交叉验证，为杀模型的准确度和覆盖度评估提供依据。

3、验模型：验模型作为反作弊系统的效果评估体系，直接与业务运营系统打通，抽取业务的关键指标，分别抽样评估查模型的异常覆盖能力以及杀模型识别准确度。此外，验模型还提供异常用户打击前后业务关键指标的波动检测。

4.1.3 反作弊模型海量数据处理能力

反作弊模型每天处理涉及用户使用行为、付费应用、社交应用、商品数据等10大领域的数据，每天处理5亿活跃终端，30亿+App启动数据，40亿+广告数据，500亿+的App行为数据。

4.1.4 适用于内外部的平台化数据服务接口

灯塔反作弊解决方案普适性强，基于SDK+API的通用解决方案，接入成本小，可覆盖渠道推广反作弊、运营数据统计质量优化、业务反垃圾、营销活动防刷、广告反作弊等场景。

4.2 业内反作弊技术最新动态

4.2.1 深度神经网络与图的结合

近十年，深度学习成为人工智能和机器学习的研究热点，在声学、图像和自然语言处理领域展示了顶尖的性能。深度学习提取数据底层复杂模型的表达能力收到广泛认可。著名的卷积神经网络（CNN）是一种常用的深度学习模型，其研究对象限制在Euclidean data。最显著的特征就是有规则的空间结构，例如，图片是规则的正方形栅格，语音是规则的一维序列。这些数据结构能够用一维、二维的矩阵标识，CNN对这些数据的处理效率很高。

但是，现实生活中有很多数据并不具备规则的空间结构，称为Non Euclidean data。比如推荐系统、电子交易、计算几何、脑信号、分子结构等抽象出的图谱。这些图谱结构中的每个节点连接都不尽相同，有的节点有三个连接，有的节点有两个连接，是不规则的数据结构。

所以，如何利用深度神经网络进行图数据分析的问题吸引了众多研究人员的关注。将传统深度学习架构应用于图结构存在如下挑战：

1、不规则领域：图像、音频和文本具备清晰的网络结构，而图结构则属于不规则领域，这使得一

些基础数学运算无法泛化至图。例如，为图数据定义的卷积和池化操作并不是直接的，而这些CNN中的基础操作。

2、多变的结构和任务：图具备多样化的结构。例如，图可以是同质的，也可以是异质的；可以加权，也可以不加权；可以有符号，也可以无符号。此外，图任务也有很多种，节点问题包含节点分类和连接预测，图问题包含图分类和图生成。

3、可扩展性和并行化：在大数据时代，实际的图数据很容易扩展成数百万的节点和边，如社交网络或电商网络。因此，如何设计可扩展模型并最好使其具有线性时间复杂度，成为了研究的关键。此外，由于图中的节点和边是互连的，通常需要作为一个整体来建模，因此如何实施并行化计算是另一个关键问题。

4、跨学科：图通常与其他学科有关，如生物学、化学或社会科学。这种跨学科的性质为图的应用提供了机会和挑战。领域知识可用于解决特定问题，但集成领域知识可能提高模型设计的难度。

深度神经网络应用于图数据的方法主要分为半监督方法和无监督方法：GNN和GCN是半监督方法，它们利用节点属性和节点标签端到端地训练模型参数，GAE是无监督方法。模型的输入是将要学习的图 $G = (V, E)$ ，经过一层一层的计算而发生变化，最后输出一个图结构，该图结构是一个节点级别的特征参数矩阵。

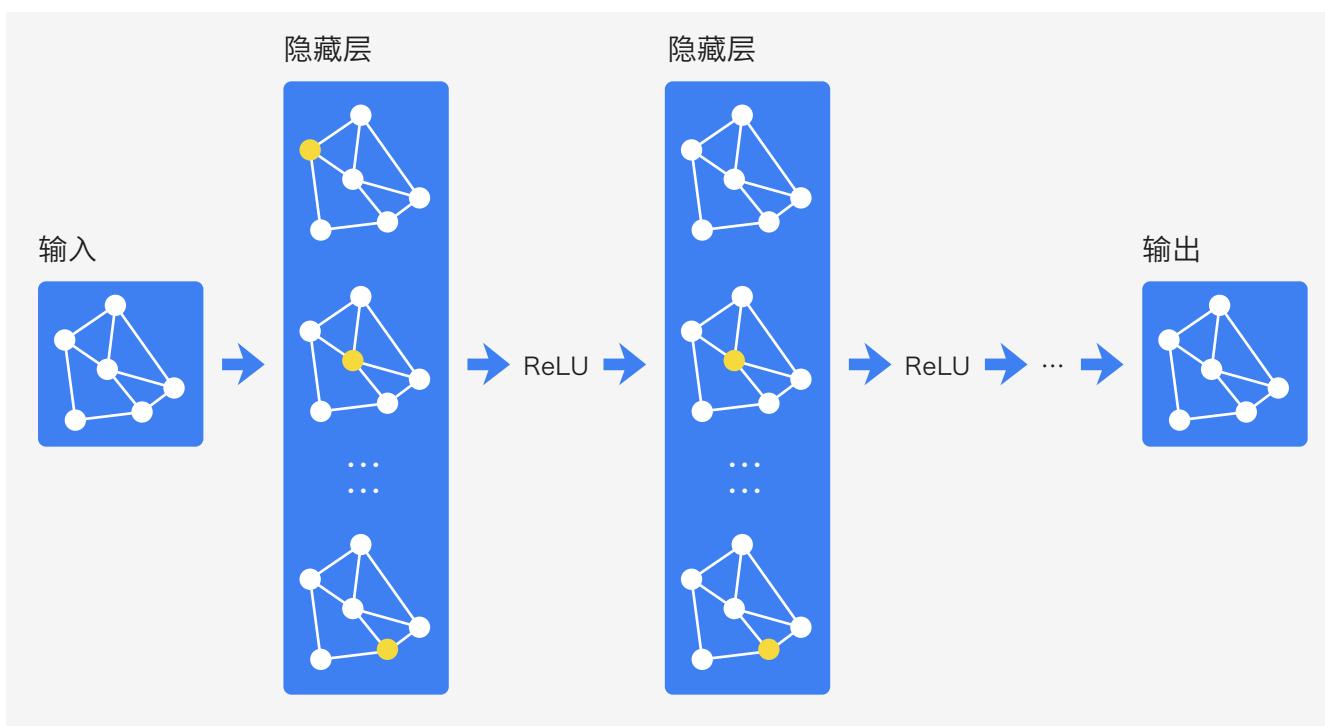


图16 带有一阶滤波器的多层GCN示意图

示例：众包作弊用户检测场景下深度神经网络与图的应用

下面结合众包作弊用户检测场景来说明图的建模和深度学习在图方面的应用。

结合问题进行图建模：以用户为图中的节点，用户的特征为节点的属性，评论过相同App的用户之间建立边关系，如图16所示。

根据图结构的特点选择模型：GCN模型能够同时对图中的节点特征信息和结构信息进行端到端学习，因此是当前场景下对图结构学习任务的最佳选择。

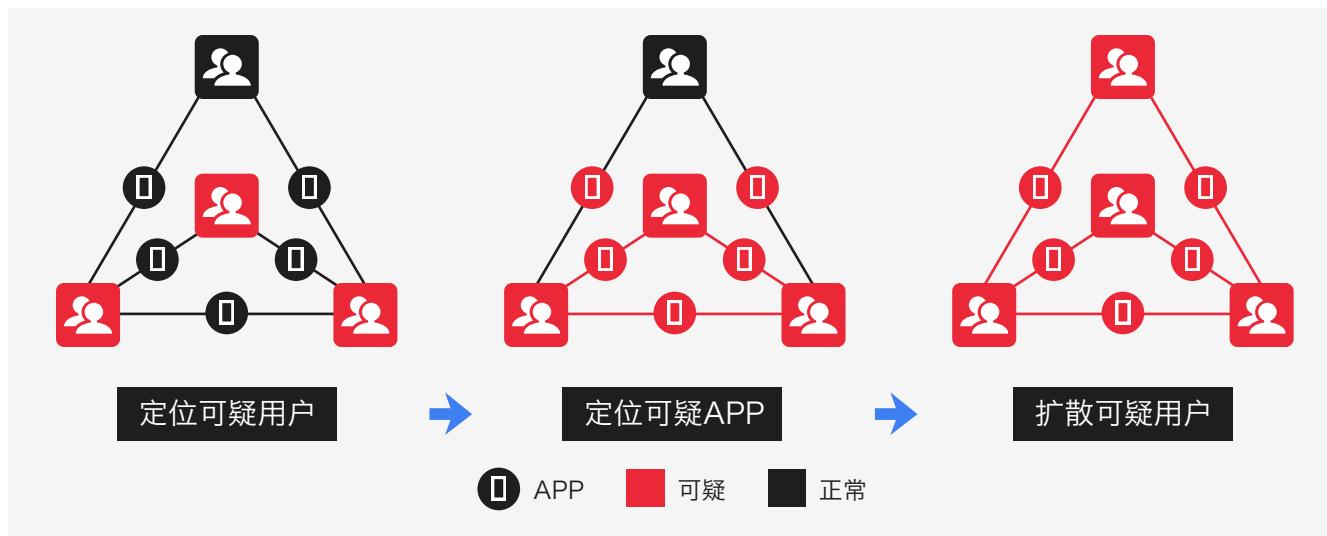


图17 基于图的众包作弊用户检测建模示意图

4.2.1 区块链技术在流量反作弊中的应用

从2016年开始，业界对如何利用各公司在不同场景中反作弊的优势共建通用的无效流量过滤方案进行深入的研究。腾讯灯塔与MMA中国共同关注区块链技术在广告行业反作弊中的应用，在多次洽谈和交流过后，形成了该技术在广告反作弊的落地方案。在此背景下，2018年7月，由MMA中国GIVT LIST工作组发起DIF (Distributed Invalid Traffic Filter) 项目，腾讯灯塔作为DIF项目黑库的最大贡献方参与到DIF项目的共建工作中。

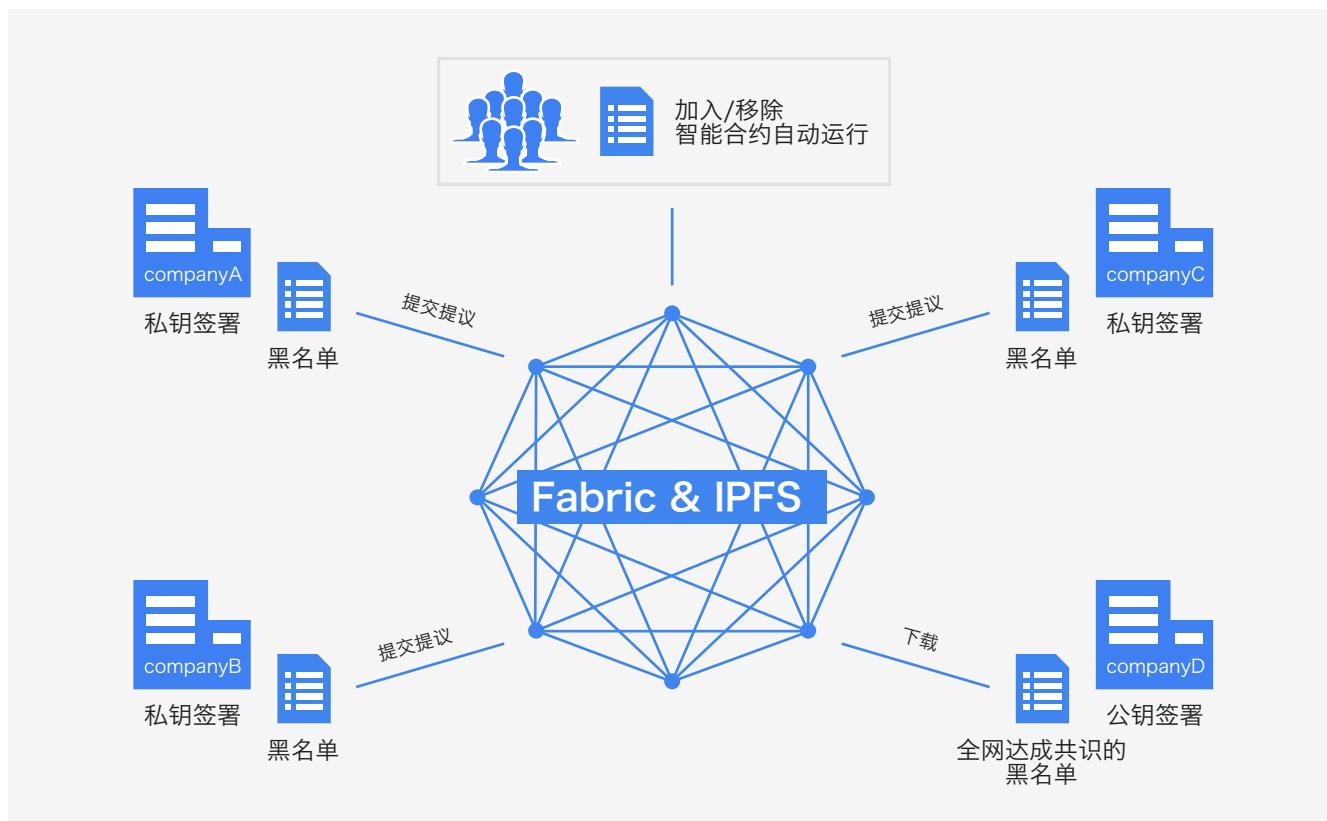


图18 DIF示意图

从图18可以看出，每个成员企业作为一个节点可以随时增量提交自己的黑产相关的数据并触发智能合约，成员可获取自身和全网合并后的GIVT LIST。例如，某成员企业提交了黑设备号并通过了合约中的背书阈值N，就可以影响联盟中其他成员企业节点获取到的GIVT LIST，DIF系统在区块链上实时记录共识、实时合并，再也无须管理员手动执行合并。同理，如果要将某个黑设备号进行撤销，同样可以由各个成员企业节点提交，触发智能合约，获得至少M个节点背书同意，全网节点将自动更新。

第五章 结语

在中国数字广告市场，无效流量的攻防战是一场持久战，随着制造无效流量的手段和技术的不断升级，打击无效流量的技术和措施也在不断更新。为了维护行业的健康发展，广告主、媒体、代理公司、第三方、行业组织等各方在防止和打击无效流量上逐步形成共识。在行业组织、行业各方积极努力下，中国无效流量监测向更加规范化、标准化的方向发展。2018年，互动广告国家标准颁布，其中包含了投放验证要求；在中国广告协会领导下，一般无效流量行业名单(GIVT list)正在制定中。腾讯灯塔和秒针系统坚持遵循MRC、CMAC和MMA等公认的行业标准，并积极倡导行业标准的实施落地。虽然应对虚假流量的“战争”还会继续，但有了行业标准、行业各方的共同努力，2019年中国数字营销生态一定会更加透明、更加健康！