



BitClave: 去中心化搜索 生态系统

白皮书v 0.9.9, 2017年12月

<http://www.bitclave.com/>

在目前的\$550B 的广告市场中，太多的资金流入隐藏的广告网络，其 对商家和顾客的附加值太少。BitClave 正使用区块链来消除广告服务“中 间商”，并创建商家和顾客间的直接连接。 在 BitClave 活跃搜索生态圈 中，顾客可以控制自己的身份，决定谁可以访问他们的数据，并在每次商 家“使用”他们的数据下订单时“得到报酬”。 BitClave 让商家与顾客有 直接关系，可以提供独特的针对性促销。 BitClave，一个开放搜索市场能 保持价格公平，消除中间商，能将全部资金为顾客和商家服务。

声明:本草拟白皮书仅供用于讨论和学习。白皮书所载的信息有可能发生变化，在经董事会、顾问 委员会和公司律师讨论、审查和修订前，本文件草案的任何部分都暂不具有法律约束力或可执行 性。请勿不带此声明复制或传播本文档任何内容。本白皮书的最终版本将在采用后尽快公布。

目录

执行概述

问题描述	5
解决方案概述	8
用例举例	9
律师和法律顾问	9
教育学位项目	9
工作搜索	10
医疗需求	11
资产管理	11

汽车销售

技术解决方案概述	13
BitClave 活跃搜索生态系统(BASE)	13
活跃搜索生态圈(BASE)的活动结构	15
示例：直接到消费者汽车营销	17
活动账本中的匿名顾客和零售商	18
示例：连接多个零售商到一系列活动	18
顾客活动代币(CAT)	19
作为参与激励的代币	19
零售分析提供商	20
技术解决方案细节	20
主要的 BASE 组件	20
注册子系统	21
REQUEST子系统	21
OFFER子系统	22
搜索服务	23
排名和匿名服务	24

按顾客ID排序	25
以顾客发起的假名排序	26
第三方参与者排名与匿名服务	27
活动分析	27
BASE 可扩展性和 BASE NODE API	29
以太坊区块链	30
储存的可伸缩性	31
交易速度	32
法律	34
发展计划	35
初期发展投入	35
早期平台用户的价值和经验	36
发展计划	36
新机会	36
融资以及代币发放	37
所得款项用途	37
筹款计划	38
代币分配	38
交易所	39
用户好处	39
团队	40
术语表	45

执行概述

BitClave 活跃搜索生态圈为顾客和商家提供了可直接交易而无需中间商的 互动平台

在网络广告中，商家不得不向“中间商”支付高昂费用以吸引受众看到其推广内容。然而，这些信息要么和很多广告放在一起，堵塞在拥挤的网页广告条中，要么直接被对方投入 垃圾邮件。商家几乎也无法保证他们的推广流量数据是否真实。实际上，近 50% 的广告流量 都是漫游器产生的，这基本上也破坏了广告的本身目的。卖家支付了“效果，观看次数和点击率”，却得到非常低的转化率，使投资回报率无法得到保障。

离线广告情况无异。通常来说，离线广告商通过群发邮件进行推广，结果无外乎就是“点击或者错过”。而成堆的邮件涌现在用户面前，使其无法成功定位，最终无法得到满意的投 资回报率。这一点和其他因素共同导致了极低的转化率。大部分推广信息被递送给了对产品毫不关心或注意力可能在其他产品上的用户。

这些效率不高的线上线下措施对整个服务价值链产生了不良影响。一旦越来越多的商家 被迫向谷歌和 Facebook 之类的“中间商”进行支付，顾客就不得不花更多钱购买产品和服务。最终，商家亏损，而顾客只会花更多的钱买到更差的产品，两败俱伤。

为了解决上述问题，BitClave 提出了一个没有中间人的系统，商家和顾客间的互动直接 由网络达成。如此一来，商家就可直接和自主地基于顾客的显性搜索,通过使用 BitClave 的去 中心化搜索应用，向顾客提供个性化的产品服务。

在 BitClave 生态圈中，顾客可以控制自己的数据，并可以选择是否向零售商显示其身份 或个人信息作为其搜索内容的一部分。同时，零售商通过有针对性的促销活动回应这些搜索 行为，其作为顾客浏览的回馈。所产生的市场可能激励顾客分享一些个人信息，但是这种类型的共享不是成功搜索所必要的。生态圈使用户能够控制自己的隐私偏好，而不像如 Google 和 Facebook 这样的“免费”服务，他们经常向经纪公司销售用户数据。

BitClave 活跃搜索生态圈准备就绪后，销售数据就是过时的事情，因为公司向顾客直接

提供促销活动，在顾客和零售商之间创造有效而丰富的市场经济。

问题描述

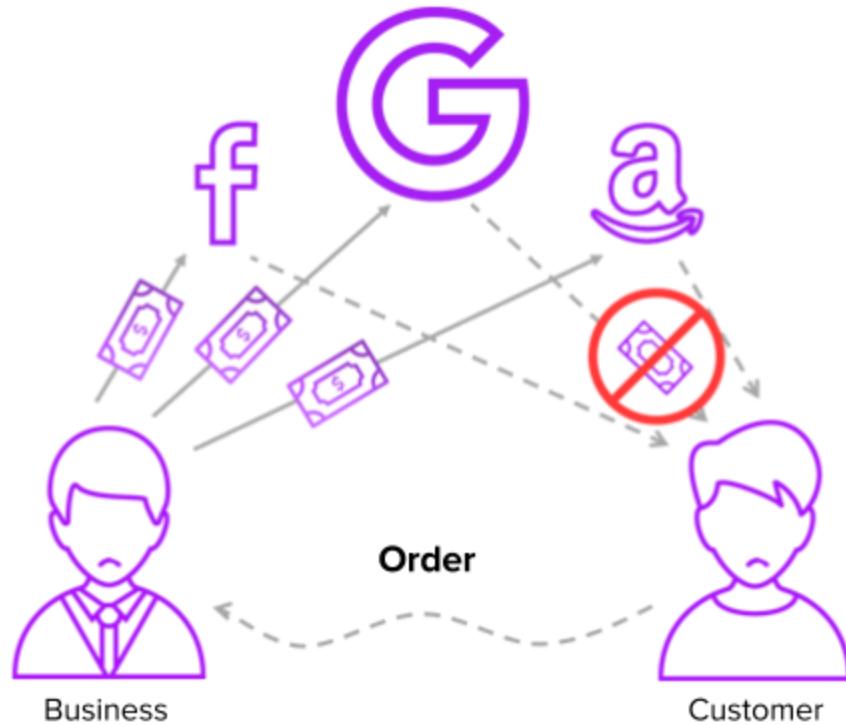


图 1:在当前的广告生态圈中，商家被迫向广告“中间商”支付大量的营销资金，后者定位目标顾客较弱，但也为其做广告的顾客提供了一点点直接的价值。对于顾客和商家而言，这是一个双失的情景，而广告巨头则在这个过程中获益颇丰。

目前，“卖家-广告商-顾客”分散价值链丧失了市场良机。

高达 5500 亿美元的广告市场¹已被打破。如今，商家和不计其数的中间人在广告堆中来回竞争。主导地位的广告公司(例如谷歌，亚马逊，Facebook)通过收取高昂费用来接触 用户。而商家没有任何保障使他们的广告转化成业务，甚至无法确知广告流量是否真实，实

际上，将近 50%的广告流量都是漫游器产生的，基本上也就破坏了广告本身的目的^{2,3}。商家支付广告的价钱越多，顾客也会花更多的钱。最终，商家亏损，顾客用更多的钱买到更差的产品，两败俱伤，见图 1。

高达 5500 亿美元的广告市场¹已被打破。如今，商家和不计其数的中间人在广告堆中来回竞争。主导地位的广告公司(例如谷歌，亚马逊，Facebook)通过收取高昂费用来接触 用户。而商家没有任何保障使他们的广告转化成业务，甚至无法确知广告流量是否真实，实际上，将近 50%的广告流量都是漫游器产生的，基本上也就破坏了广告本身的目的^{2,3}。商家支付广告的价钱越多，顾客也会花更多的钱。最终，商家亏损，顾客用

¹ Statista, “全球广告市场 - 统计 & 事实”，可用 <https://www.statista.com/topics/990/global-advertising-market/>, 2017 年 6 月 15 日

² Incapsula, “机器人流量报告 2016”，可用 <https://www.incapsula.com/blog/bot-traffic-report-2016.html>, 2017 年 1 月.

³ G. Sloane, “Nearly 25% of Video Ad Views Are Fraudulent, and 6 Other Alarming Stats”，可用 <http://www.adweek.com/digital/7-things-you-need-know-about-bots-are-threatening-ad-industry-161849/>, 2014 年 12 月

更多的钱买到更差的产品，两败俱伤，见图 1。

大型在线广告公司同样错过巨大的市场机会，因为他们没有动力来优化卖家-顾客价值链(即转化)。相反，这些公司通过提高理想的广告展示位置和点击率的价格来不懈地努力最大化自己的利益，同时在分散的专有的广告网络的围墙花园后囤积用户数据。

当今的集中的广告网络阻碍了市场的增长，因为它们没有为卖家对顾客转化而得以优化。

全球市场要求尊重顾客隐私。用户数据有自身价值但非免费品。

大型在线广告公司也面临着保护顾客隐私的监管压力。最近，欧盟(EU)对“电子隐私权指令”以及“通用数据保护条例”(GDPR)作出更改，突显了政府要求技术公司维护顾客隐私权的新趋势。

众所周知，可操作的顾客数据具有内在价值。允许顾客控制自己的数据并提供激励措施使他们以受控制的、尊重隐私的方式使用区块链分享数据，为顾客创造了新机会，而且也是合规的。

为实现大型顾客数据集的匿名搜索，全球市场的隐私规定是关键的近期驱动因素。

广告简史：扼杀创新的市场定将面临技术破坏。

自古以来，广告一直是商业运作环节中一大重要组成部分。印刷技术是现代社会的一项重大发明，它在全球范围的传播使内容出版成为一种新的宣传媒介，但若没有内容营销，印刷技术便是不完整的。

广告的历史和演变不仅记录了，也在极大程度上推动了通信技术的发展。就如黄页，为商家提供的打印电话簿，就借着广告商的资助将电话通信扩展到了商家范畴。

互联网的兴起加快了广告的覆盖速度，也改变了人们对广告的看法。事实上，雅虎在以前就作为互联网入口点，扮演着许多黄页的数字模拟器，而目前是互联网登陆页的桥梁。

虽然广告媒体越来越高效，但广告的核心功能，即人们与服务之间的关联建立却鲜有进展。搜索和社交媒体虽然在面向顾客的服务中十分突出，它们对大规模高性能知识和社交图

表的透明化也有革命性的作用，但仍然和雅虎及黄页之前的商业模式大同小异。由于在线广告的目标是连接商家与相关顾客，服务提供商和商家会在广告曝光量，网页浏览量和点击率花费营销预算的大部分。这种方法只能较松地转化为业务销售或顾客价值。这主要是由于流行的“免费”网络服务和隐藏的广告网络的暗网相结合，导致双方之间广泛且昂贵的沟壑。我们认为“中间人”的广告模式不仅是不必要的，而且对商业价值和

声誉作用不确定。

广告业演变的下一步就真正具有革命性了。区块链是一个强大且新兴的技术，在不需要中央权力参与的情况下，它能使互相不信任的双方投入到互惠共赢的共同事业中去。我们认为基于区块链的系统非常适合使顾客和商家通过整个推广-购买价值链而在互利的市场活动中直接连接。作为紧密联合人与商家的媒介，广告业发展的下一阶段就是去中心化搜索。为了使人和商家投入到价值创造中去，BitClave 采用这些强大的设计模式来重新设想一个更加透明又富有意义的媒介。

通过过去中心化搜索，以前浪费的广告费用将被重新定向于推广活动，其将吸引对正在销售的产品和确实符合顾客需求的奖励方案真正感兴趣的顾客。通过精心设计的区块链系统，顾客资料可由隐私侵入性元数据(由第三方拥有和控制)提升为顾客拥有的搜索元数据，并仅在与搜索相关的情况下选择性显示，创建一个隐私友好的市场，其中顾客和商家分享价值创造。通过在公开的区块链中以保护方式存储顾客数据(即提供匿名性和选择性数据共享)，新形式的奖励和忠诚方案得以产生。

广告业因技术产生的破坏而再次成熟。 BitClave 技术可以实现 1)可扩展的数据集搜索; 2)数据隐私和顾客匿名; 以及 3)参与广告市场的激励。

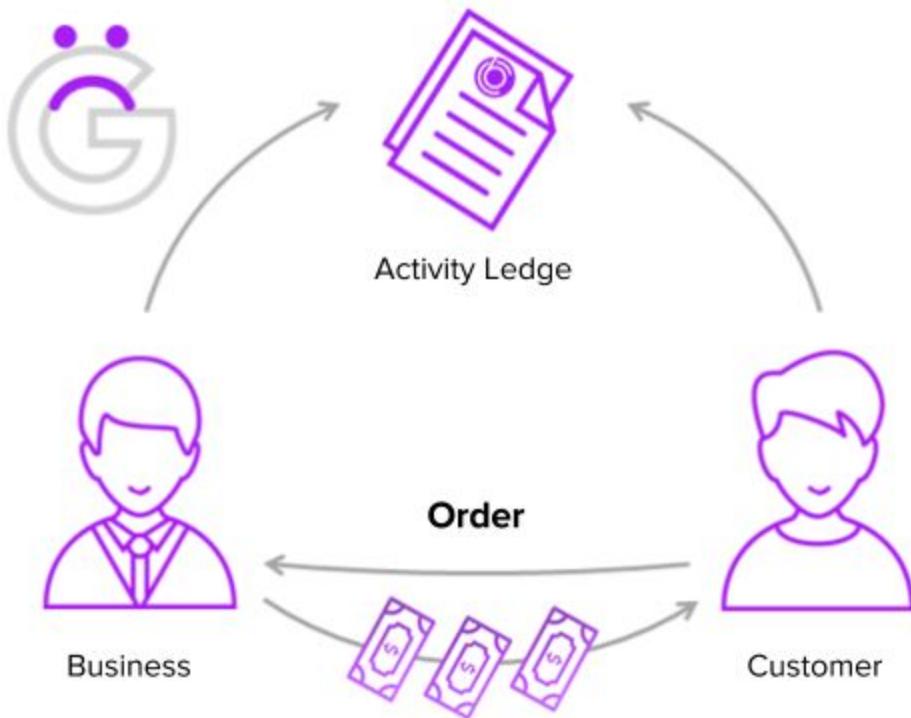


图 2:在 BitClave 活跃搜索生态圈(BASE)中，商家直接向顾客搜索与在售的商品和服务相匹配的顾客推广。顾客可以通过与直接有针对性的广告进行交互而获得 CAT 代币，同时商家获得更强大主导顾客。BASE 活动分类账促进了整个匹配过程，前者保护私人顾客数据并允许选择性数据共享。

解决方案说明

BITCLAVE 的去中心化搜索生态圈通过顾客到商家价值链实现了空前的市场效率。

去中心化搜索的愿景是通过支持分布式的、以顾客为主导的对区块链上的顾客活动的收集来实现的。BitClave 使用在匿名活动账本中收集的在线数据以及顾客直接发布和维护的个人资料和偏好设置，为需求驱动的营销和零售创造了一个所有各方进入门槛较低、基于代币的生态圈。这个生态圈利用传统在线广告的优势、广泛的生成和共享用户数据的能力以及互联网的远程到达，但是消除了数字广告领域传统上存在的障碍，即侵犯隐私、不受信任的数据来源以及昂贵的第三方广告网络。BitClave 的解决方案使各类商家都能够参与开放的生态圈。我们创新的去中心化搜索技术是由市场所驱动的，意味着商家可以通过实际效果优化营销投资、顾客得以受激励参与、匿名和数据隐私为每个个体参与方所掌控。如图 2 所示，该生态圈为顾客和商

家创造了双赢局面，同时消除了对广告中间商的需求。

Bitclave 第一次实现了卖家-顾客价值链的最优化。在 Bitclave 活跃搜索生态圈 (BASE)中，市场经济驱使了数据分享的动机，该动机适当地平衡折中了市场效率和个人隐私。数据依然包含巨大的价值，但顾客和商家则有能力选择是否分享这些数据。通过取消强制的数据分享和来自现今巨大的广告网络对策的收益，每一方都能赢利。Bitclave 的公开 BASE 生态系统保证了技术持续发展的同时创新在广告业也能持续进行。

使用示例

基于 BASE 平台建立的革命性应用的潜力十分可观。为了强调 BASE 的结构和潜在优点，我们混合了线上线下要素，阐述了一些实例用例及在自动化零售领域的详细的用例研究。 我们用例的选择倾向于用“每次点击成本”数据来展现，此数据相当于每次用户点击广告时

商家应向谷歌支付的费用⁴。最昂贵的关键词，包括“律师”，“保险”和“学位”，不管点击者是谁或其是否会继续关注此业务，每次点击都处于 45-60 美元的范围。围绕个人信息的收集对高质量的目标服务十分重要的主要思想，每个例子会进行得更深入。因为个人信息会以各种渠道被投进 BASE，包括通过用户注册过程及作为搜索请求的一部分，我们特别强调匿名化，数据保护及顾

律师和法律顾问

由于法律案件独特且多样化的特性，个人数据的分享在为岗位搜寻合适的专业人员过程中是决定性的。每个个体案件都有大量有细微差别的信息，人们要联系所有细节，且对律师来说，尤其在一段关系的初始阶段还要得到足够的信息来做理智的决定，而这是很有挑战性的。在这种情况下，个人数据可帮助法律专职人员决定他们是否适合一个潜在的客户。BASE 支持用户受保护地公布个人信息和交易历史，这样用户随后即可选择分享选择的信息，同时受潜在的法律专职人员的保护。如果特定的用户数据对该法律人员有用，用户可选择向他们展示数据而不用将其公示。该信息可进一步让法律人员锁定更多理想客户，并为他们定制提供的服务。

教育学位项目

在一个教育机构们推销相似的特点及优势的拥挤的市场里，一个潜在学生很难发现最合适学校。有可观广告预算的最大型的大学在广告空间上出价比更小型的大学要高，这些小型学校也许会失去联系能与之完美契合的学生的机会。在更高等的教育机构努力达到招生指标的同时，学生们则会遗漏能帮助他们做正确选择的信息。学校目前转向了一种新技术来发现能适应学术和学校整体概况的合适的学生，他们希望招到其感兴趣的学生并花费数千美元来广告宣传。假设一个学生将从高中毕业，正在寻找离家乡不远的大学里的生物项目。他们用 BASE 可以搜索生物学位项目，且已在他们的 BASE 档案中私密存储的信息可以指导潜在大学的

⁴ E. Gabbert, 广告世界里最昂贵的 25 个关键词-2017 版”，2017 年 6 月，<http://www.wordstream.com/blog/ws/2017/06/27/most-expensive-keywords>

招生协调人对他们进行回应，并告知该高度相关的项目的细节，而非找到在广告上花费最多的机构。与第三方网络不同，BASE 会根据搜索的选择性分享最相关的信息的能力，来为学生和学位项目创建更相关的联系。如今，学生可以选择接收由 BASE 辨别的个性化广告，挣得 CAT 代币来进一步支持搜索，或者如果学校支持的话，他们甚至可以支付项目申请的费用。更重要的是，因为学生收到了有特定目标的广告，他们会知道该学校对他们的申请感兴趣，同时会增强他们进行配对的信心，并促进一段有利的关系的开始。

工作搜索

类似于对寻求深造的学生的配对的用例，BASE 也可被用作一个工作搜索平台。求职者可以利用 BASE 去中心化搜索平台来搜寻雇主，同时雇主也可找到有特定技能的潜在雇员。在超竞争技术工作领域有特殊意义的 BASE，可被视作“反工作搜索”的一种类型，即求职者可匿名公开职业兴趣和主要技能，雇主则锁定特定的职业兴趣来对为求职者定制的工作岗位进行宣传，从而匹配商家需求和雇员的独特技能。这与传统工作搜索栏形成了鲜明对比，在后者，雇主们公布统一的“软件工程师”工作岗位会导致公司内部的员工流失率。

医疗需求

数百万计的人每天都会面临许多不同的医疗状况。对待处理这些状况需要医学专家和多种设施仪器的帮助。医疗记录和个人病史的私有性会让进行研究和联系专家富有挑战性。许多人不想将私密信息与公共的线上用户联系在一起，在为医生进行调查或者分享病史时犹豫不决。使用 BASE，病患可以私密且安全地为符合独特需求的医疗人员进行调查。病患搜寻一个特殊病域时会从相关的医疗人员与医学专家处找到一系列答案，后者有服务提供的描述或者有符合搜查病患的服务提供。

资产管理

许多上班族都在思考如何管理退休金。然而个人财务记录是高度保密的，许多人都不习惯通过不安全的渠道提供该类信息。没有个人的私密信息，资产管理人、财务计划师和贷款人员向潜在客户提供最准确的信息会有挑战性，这样会导致双方的机会损失。寻找财务计划师的个人用 BASE 可以搜寻专属于特定收入范围或投资策略的公司，仅仅将关键的个人财务指标展示给符合个人标准的公司。商家将对财务计划公司的搜寻反馈结果，前者已把个人作为理想客户，当个人与提供的服务相互影响且个人选择参与进来，通过受保护的 BASE 平台分享各自的信息时，商家会定制且个性化其服务提供。

汽车销售

我们将更详细地描述汽车销售用例，因为此提供了我们 BASE 平台解决几个独特的挑战。正如在许多行业，客户获取是关键业务和昂贵的销售组件。在汽车经销商行业，这个因素是运营成功的分销网络的关键。汽车经销商通常通过推广通用在线转介来源（如 Google AdSense 或 Facebook 观众网络）和面向流行客户的汽车信息和定价服务（如 TrueCar）的面向经销商的产品，与汽车销售商合作，花费高达 200 美元，针对线索的重点网关比通用网关更昂贵，更有效。

他们通过国家、地区和地方的关键词与其他经销商竞争，以及与租赁、保险和融资等其他汽车相关服务。这种数字广告与传统营销相结合，包括本地播客、广播、广告牌和赞助。传统的区域经销商协会也得到了支持。

，当地的经销商将营销资金汇集在一起，以提高特定地区的广告购买效率，以及汇集数据资源，如客户购买历史。所有这些都增加了一个昂贵，复杂，竞争激烈的环境。一个持续供应而不是需求的环境。因此，即使新车销售的整体利润下滑，客户收购的成本也有所收窄，从而削弱了经销商成功运作的能力。这种成本压力只会因车辆的快速折旧而加剧。

在实践中，几百美元通常是失去的领先者或快乐的客户离开新车之间的门槛。今天，汽车经销商提供100美元的预付卡或6个月的路边援助服务，以帮助交易此外，这些“交易甜味剂”是以汽车为重点的转介服务为汽车经销商自己提供的，作为奖励他们高成本的理由。在销售和满意的客户方面，用于收购潜在客户的预算花费在向客户提供的直接促销优惠上。 BASE平台，促进直接客户对企业的参与和天生审批导致的质量，恰恰是浪费重定向目标支出增强客户关系的解决方案。

在BitClave生态系统中，使用图3中的移动应用程序模型进行了说明，汽车经销商将有机会使用精确的数据驱动定位向潜在买家显示他们的促销和广告。同时，经销商将保证他们的内容被合法的买家观看，而不是对内容不感兴趣或机器人随机方。经销商可以选择通过各种因素过滤潜在客户，包括拥有两年以上车辆或最近达到法定驾驶年龄的年轻人等。

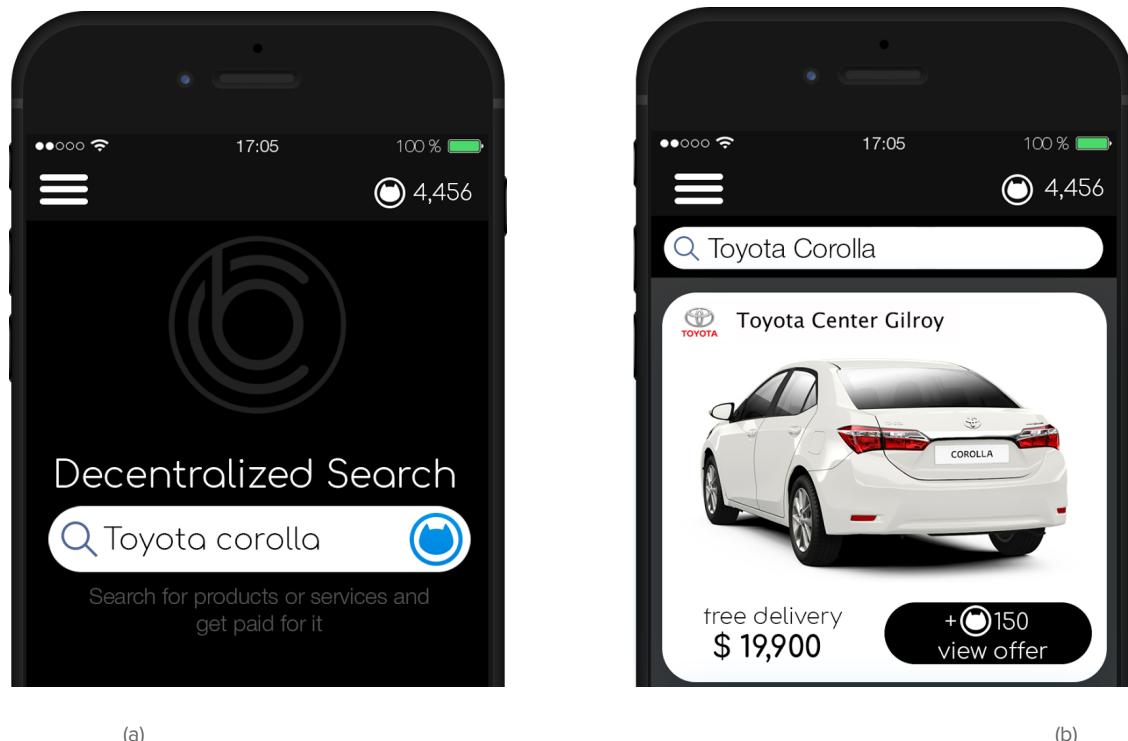


图 3:在移动设备上的 BitClave 去中心化搜索应用的概念包括:(a)一种流线型的搜索界面向用户展示他们挣了多少可以在 BASE 系统中使用的 CAT 代币。在搜索了一个产品或服务之后，该应用会展示(b)提供 CAT 激励的潜在报价 以查看报价的细节。

对在 BASE 中使用活动账本来记录他们和客户之间合作的经销商来说，最主要的一点好处是，客户的购买历

史和喜好的相关数据会很安全地被存储在账本中。这些数据能够为 经销商营销团队提供有价值的见解，包括什么时候重新给先前的客户投放广告，什么时候 提供打折服务，或是客户对什么类型的附属配件感兴趣。存 储在 BASE 账本中的数据可能 会进一步表明客户的“评级”，这是与广告互动频率和相关转化率有关的。有了 这些评级， 经销商可以评估广告对每个客户的价值，并以此来优化他们的广告战略和投资回报。举个例子， 如果客户看广告和促销活动的频率很高，但是在看了之后转化率很低，那么由于广 告和促销活动导致顾客购 买的机会很低，商家也许会进一步减少面向这类客户投放广告。 同样的，随着时间分析客户行为可能会使经 销商得知哪种促销活动成功让他们既节省了成 本又提升了服务和促销活动质量，并且使投资回报最大化。这 些例子证明了即使在复杂且竞争激烈的汽车销售领域，BASE 平台在传统广告模式上所发挥的价值。

技术解决方案概述

Bitclave 是位于加利福尼亚 Mountain View 的创业公司，提供无缝的客户奖励和支付解决方案。

Bitclave 致力的一个首要创新点是基于区块链的分布式系统，即称为 Bitclave 活跃搜索生态系统(BASE)。在这里，顾客活动代币(CAT)激励着每一个 BASE 系统的参与者。

BASE 和 CAT 最初的版本是基于以太坊技术的——一个利用智能合约的开源且基于 区块链的分布式计算平台。这些加密、安全的智能合约是存储在以太坊区块链上有状态的 应用程序，它完全有能力执行程序。虽然以太坊是最初的目标，但如果合适的话，我们也 有可能会转移到其他不同的区块链技术。在接下来的章节里可以看到更多关于潜在的替代 区块链技术。

BitClave 活跃搜索生态系统(BASE)

BASE 依赖区块链来实现对在该生态系统中大量客户活动数据的存储和管理。这些活 动是由客户自己和与他们交互的零售商操作的软件端点创建的。因此，包括零售网站和营 销板在内的软件应用可以从区块链中读取和写入;例如，这些一体化应用程序可以被用来 建立基于客户偏好和共享人口信息的有价值的受众匹配知识，或者了解提供特定产品的商 家。由于 BASE 生态系统是去中心化和开放式的，任何一个人都可以创建这样一个软件用 来与在区块链中公布的客户和商家数据互动。商家和客户没有发布和售卖这些数据给大型 广告服务提供商。相反，他们通过用户进一步控制访问权限控制了他们贡献给区块链的数据，而不仅仅是这些数据是否被公开共享或者加密保护。

特别注意，面向用户的软件有使贡献给区块链的信息匿名化的能力。这会创建我们所说的匿名活动账本。活动匿名化是由只允许有授权的一方把多个活动归因于同一客户的方式完成的。对于其他各方，数据不会归因于特定的个体(或超出一定时长的链接)，而在统计和数据汇集的目的上保有其价值。通过使用区块链和智能合约，客户可以控制哪些数据被允许创建、共享和访问。

由于匿名活动账本是 BASE 零售基础设施的基石，提供了去中心化能力，用于描述匿 名客户和零售商活动的众包和共享数据，它促进提高了各种来自于客户、商店、移动应用、 网站和其他不同零售领域的分析能力。如前文所说，任何一方都可以给活动账本贡献(潜 在匿名)数据，任何一方亦可以从数据中获取价值。这取决于贡献者是否对数据进行了加 密或遮掩。相似地，给定的数据资产的价值(CATs 的价值)可以被客户、商家、第三方服 务提供者或由智能合约明确规定了某些组合所拥有，而用户可以保留对使用和公开个人可 识别数据的控制权。

用户可以通过多种不同方式向活动账本贡献数据。他们可以发起一份概要，它包括个 人信息，例如人口统计(年龄、收入等级、居住城市/地区)、搜索偏好、兴趣以及他们认 为与搜索相关的任何额外信息。此外，当一个用户发布这样的信息时，他们可以选择将其 干净(所以它是完全公开的)发布或者被加密保护发布。这可能

会允许他们将他们的个人信息有选择地透露给一些零售商，而不是所有。

额外的数据来源包括

-通过面向用户的应用程序搜索商品和服务的历史，每个搜索查询都被发布到区块链上。

-搜索产品或服务的客户和提供这些产品或服务的提供商之间的实际业务交易。

再次说明，用户可以配置如何在搜索查询中显示或保护信息，例如匿名化他们的身份

或对搜索项和元数据字段应用加密保护。

除了显性搜索，用户还可以通过授权按钮间接贡献访问网站相关的活动数据。这与“登陆 Facebook”按钮相似，授权一个第三方网站，使用他们的 Facebook 凭证来认证/授权一个用户。例如，用户在他们最喜欢的零售网站上浏览，可以通过点击“在 BASE 中记录我的访问记录”来为这次活动创建一个记录。这个按钮由零售网站设置主持，并代表他们将浏览活动发布在活动账本上。这类活动分享仍然由客户控制，单击按钮“选择参与”将此次活动分享到区块链上。因此，该功能将依赖于合适的身份验证和授权协议，如 OAuth。这样可以确保零售商在没有用户准许的情况下无法发布浏览活动。

活跃搜索生态圈(BASE)的活动结构

为了让活跃搜索生态圈(BASE)中的活动对各方都有益，发布在账本中的活动入口应遵循标准格式。虽然此格式的正式定义将会在之后确定，但每个活动入口应至少包括(1)一个活动标记来标识入口的种类，(2)用户的唯一标识符(如用户公钥的哈希值，或者合适的匿名替换者)，(3)描述活动种类需要的任何细节，以及(4)一个时间戳。将会提供被支持的活动种类和对应元数据项的初始串列，但是活跃搜索生态圈可以随着生态圈的扩展而自由定义和引入新的活动种类。初始活动种类的示例包括：



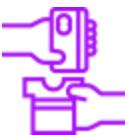
REQUEST

面向顾客的软件可以公开购物偏好、感兴趣的的商品或者个人偏好，以反映购买商品和服务的意向。一个支持 REQUEST 的元数据的示例是购买行为的时间框架，它表明了搜索行为的过期数据/时间。



OFFER

面向零售商的软件可以为降价商品或服务发布短期的促销，根据 REQUEST 中的活动，可以决定公开发布或者面对特定目标客户发布。OFFERS 能包括与 REQUEST 相似的元数据，例如展示限时促销。



VIEW

面向顾客和零售商的软件互动，面向顾客的一方发布一个唯一的证明(已读证明)来证明顾客已读报价，商家也对相应正确 OFFER 的证明进行了验证。一个已确认的 VIEW 事件将会在顾客读取 OFFER 时，触发顾客活动代币(CAT)奖励，奖励来自零售商。



BUY

顾客软件可以发布一个活动来表明用户已经在某一特定零售商处完成了购买，可能包括购买项目、价格、卖家等的描述，其中任何一种都可以通过加密保护进行选择性访问。



SELL

零售商的销售点软件可以发布一个活动(可能与用户的购买活动相对应)以表明完成了一笔交易，可能包括类似 BUY 活动的详细信息，同样也注明了任何或所有数据字段都可以通过加密保护进行选择性访问。

请注意，某些活动(如 BUY/SELL)虽然表明有对应的活动，但不一定会与其成对出现，因为任意一方都可以选择不将各自的活动发布到账本上。关于活动的基本格式说明，请见下列表格，其中右列包含了对每个字段的描述。

Activity:	<act_tag>	Tag used to reference this activity from elsewhere
Originator:	<cust_tag>	Anonymized tag used to reference activity originator
Activity	<activity_type>	Activity type, e.g., REQUEST, BUY, SELL, etc.
Activity details:	<list-of-details>	Details of activity (e.g., what was purchased and for how much)
Timestamp:	<time>	Time that activity was observed (using UTC or similar)

图 4:作为区块链入口发布在账本中的活动包含各种信息，例如活动编号，识别活动创建者身份信息的标签(可能匿名化)，以及与活动相关的细节。

为了说明活动数据格式，我们演示了在对新汽车进行在线搜索时将创建的潜在活动区块，其中<angle brackets>用于指示可能被加密或受其他保护的字段。

Activity 4E773C91	Activity 36EA9801	Activity 4E773C91
Organizer: <A>	Organizer: <A>	Organizer: <A>
Activity: REQUEST	Activity: VIEW	Activity: BUY

Activity details:	Toyota Corolla	Activity details:	PoV code: 0x236831156	Activity details:	QR code from dealership
Timestamp:	1496318700 UTC	Timestamp:	1496318885 UTC	Timestamp:	1496318943 UTC

图 5:账本中的活动入口示例，包含了对新车的搜索请求，浏览了目标广告的潜在顾客，和一个顾客的购买行为。每个活动都包括(可能匿名或受其他保护的)有关交互的入口。

相关活动本身(比如搜索行为，广告投放，访问经销网站，购买行为)已经为汽车经销商公司及其当前或未来的客户提供了有用的顾客数据。尤其是即使不明确顾客的真实身份 或他们搜索或访问网页的特殊详细信息(或在匿名账本中，以随机数字取代这些信息)，参与者仍可以用活动种类和时间戳字段来展示基本零售分析，如相对广告投放的购买量 (一个代理的广告转换率或顾客对经销商的看法)。活动区块中的其他入口和数据可以被加密或者匿名处理，来保护身份信息或其他敏感数据。

这一汽车经销商与有意购买新车的顾客之间的直接营销示例演示了 BASE 和匿名活动 账本启用的 B2C 交互。我们将进一步详细说明这个示例，以演示这种交互如何在一个端对端的示例中发挥作用。

示例:直接面向顾客的汽车营销

如下所述，直接营销可以利用潜在顾客所创建的详细 REQUEST 活动。零售商可以对 发布在账本上的大量 REQUEST 进行分析，由此来识别潜在顾客的匹配，并创建直接面向 顾客的宣传广告或促销(使用 OFFER 活动)。为启用与顾客的 REQUEST 所匹配的 OFFER，他们可以与零售商缔结一份智能合约，合约可激励顾客观看广告、访问商店(比如进行试 驾)，或者进行进一步的零售商与顾客的互动。从零售商的角度来看，相比于出钱雇佣广告商，提供这些激励措施成本可能要低得多，而投资回报率却更高。

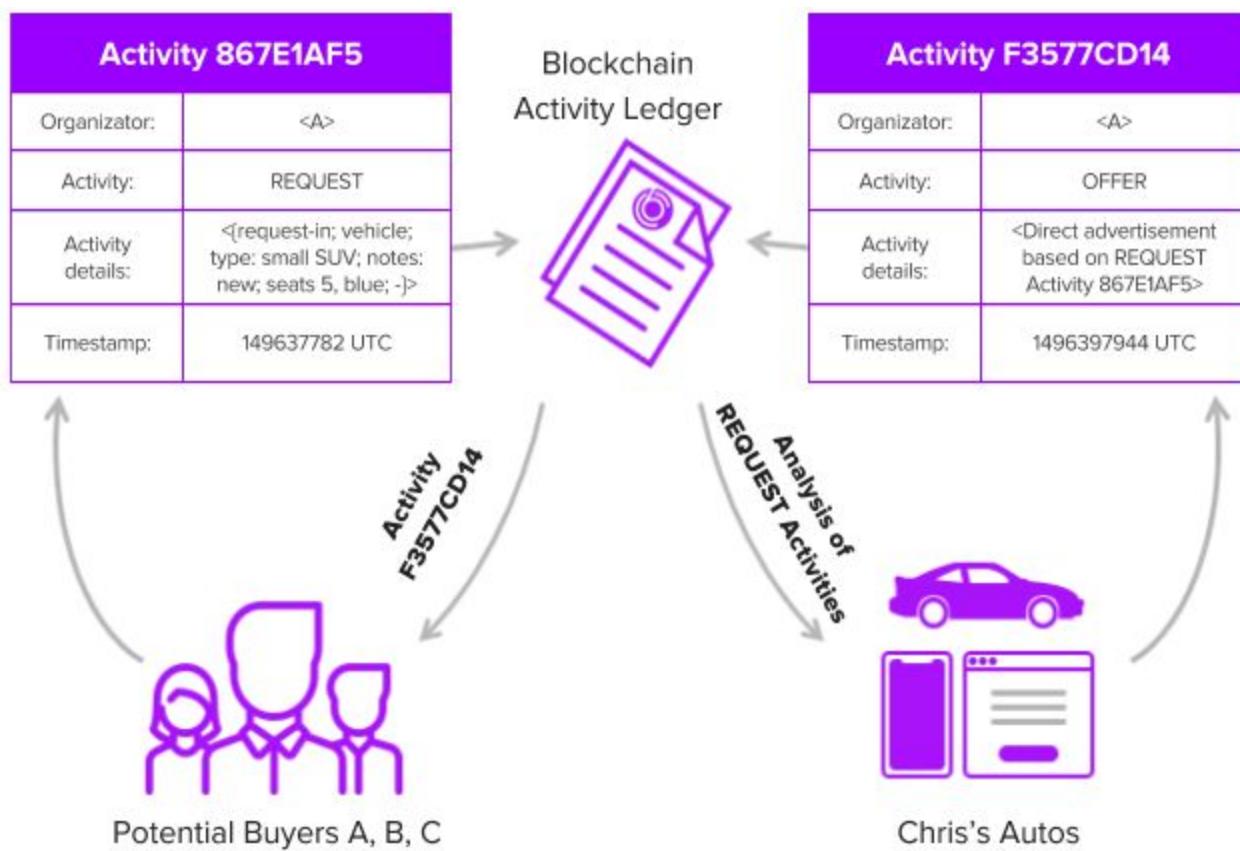


图 6: 我们演示了活动账本中潜在顾客和汽车经销商之间的信息流，包括代表客户搜索的 REQUEST 活动和代表经销商目标广告的 OFFER 活动。

活动账本中的匿名顾客和零售商

如上述，一些 BASE 中存储的顾客和零售商信息应被匿名处理，由此来保护顾客的身份信息、他们认为的敏感信息，以及他们的整个搜索历史。首先我们将叙述与匿名活动相关的可能性、角色和挑战，后面的部分将提供进一步的技术细节。

在较高的级别，匿名可以通过允许单个用户使用各种不相关的假名或备用身份，并发布到 BASE 活动账本上来实现。我们注意到，已经有许多区块链平台支持使用多个身份，任何顾客都可以创建任意数量的账户、钱包或公钥标识符；这在像比特币这样的数字加密货币平台上已经很常见了。

有几个原因，除了隐私之外，用户可能也想要这样做。例如，假设用户在购物时使用 BASE 来满足业务需要，也用于个人需求。如果这两个任务都是使用相同身份执行的，就像今天通过单片广告网络所做的那样，这两种角色会被合并到一个“顾客配置文件”中，因此用户将会看到与他们的业务和

个人生活都相关的广告。但是,如果用户可以根据不同的假名身份创建两个独立的角色,那么搜索活动就可以有效地隔离彼此,从而允许用户根据其当前角色来区分所看到的广告。虽然使用不同假名的方法消除了顾客对匿名化的担忧,但它也给商家带来了一个挑战,即现在商家需要一种方法来获知使用两个不同假名的服务请求实际上来自于同一个人,这样商家才不会发放两次奖励。这一问题的解决方案稍后将在文档中介绍。

在更一般的意义上,面向用户的软件可以支持对用户的搜索活动使用多个假名,用以支持如上所述的多个角色,也可对每个促成账本的活动使用不同的假名以真正地使用户的搜索匿名化。即便如此, BASE 也支持允许用户稍后选择性地揭示关于这些匿名发送的信息的能力。具体来说,元数据可被包含在能稍后用来揭示用户真实身份或揭示不同假名间链接(即使不公开用户的真实身份)的活动的领域内,值得注意的是,这两者都可对于一个特定的授权方列表选择性地允许。稍后的部分将提供更多的有关这些匿名化和选择性链接能力的技术上的细节。接下来的例子强调了一些有关识别和追踪的关键细节,这两者都是 BASE 默认进行阻止的。

示例:链接多个零售商的一系列活动

我们通过一个场景示例来突出账本中通过匿名化或者匿名链接活动可以得到的益处。假设有人被卷入一起严重的车祸,作为结果他们需要去找一个律师、一个新的汽车保险商、一个脊椎按摩师,以及一个汽车维修库。用户通过 BASE 来搜索相关的服务提供商。对于每个搜索,用户向账本发布一个 REQUEST 活动,每一个都使用不同的假名而非他们的真实身份。然而,许多这样的提供商可能会为各自的服务提供更好的价格——倘若他们知道顾客正在寻求的其他服务。例如,向一个汽车保险提供商认购,则可能会得到有折扣的汽车维修。更重要的是,如果服务提供商可以将许多活动链接一起,来了解用户面临的独特情况(在这里是试图从车祸中尽快恢复),他们就可以更有信心让他们给用户的 OFFER 转换成销售。因为这种对于强势领先和预期销售的信心,供应商甚至还可能会根据这些活动的共享链接而选择向用户给出一个更强势的 OFFER。

顾客活动代币(CAT)

在这个分布式活动数据收集系统之上, BitClave 正在引入一种代币,称为 BitClave 顾客活动代币(CAT),让各参与方在 BASE 生态系统内部使用。CAT 代币将被用于促进系统里可用的 BASE 中各类服务的奖励。基于 CAT 的市场将权力投放到商家和顾客手中,而非将权力集中到秘密收集顾客数据并盈利的大型广告公司上。顾客和零售商可以通过透明的、拥有顾客授权的信息发布和数据包在公共区块链上进行直接交互,其余各方亦可通过创造诸如对区块链上的数据进行操作的数据分析这样的软件功能来作为服务提供商参与贡献。

BASE 为商家和顾客解决了一个真正的问题。商家和顾客是主要的参与者,他们得到了 BASE 中多数的利益。除了商家和顾客之外, BASE 也为其他许多作为服务商的参与者提供了位置,例如搜索服务、排名服务、分析服务,都会在 BASE 经济中获益。以下部分将详细描述每个 BASE 生态系统中活跃的参与者能从中获得的激励。

作为参与激励的代币

作为支持 BASE 生态系统中交互的基础，促成活动账本的数据至关重要。因此，任何有助于账本的活动都对作为零售市场的 BASE 有潜在价值。然而，用户贡献的 REQUEST 数据是否可以直接得到 CAT 的奖励，取决于零售商是否选择用 OFFER 回应用户，而这又取决于其他用户搜索发布的 REQUEST。因为 BASE 的本质是开放的，故对这些 CAT 奖励 存在着竞争的本质观念。例如，假设两个用户 X 和 Y 对同一件产品发布 REQUEST，但是 Y 在其 REQUEST 中提供了更多配套的个人信息。由于更多的信息可能意味着更强大的卖家信心，而一个 OFFER 将转换成销售，则 a 卖家可能会向 Y 发送 OFFER 而不是 X，或者 他们可能会向 Y 发送比 X 的更有价值的 OFFER。在这种情况下，虽然没有顾客因为他们的数据得到直接的支付，但 Y 有意识地决定透露更多信息，使得他的搜索对零售商更有吸引力，因此更有可能成功。这样，BASE 更直接地代表了自由市场经济，这是因为，向账本提供不同类型的活动数据的相对价值，是由系统的市场经济状况间接决定的。

零售分析提供商

BASE 市场的独特性为买卖双方之外的其他角色创建了机会。因为 REQUEST 和 OFFER 活动可能依赖于对各种顾客和零售商的一些了解，实体就可作为分析提供商的角色 参与到 BASE 中。以这个角色，实体可以创建并向 BASE 中的各种客户销售定制的分析功能，在拥有商业产品及其服务的同时，有效地将市场扩展到支持服务。这就使得 BASE 成为了任何电子商务公司的市场营销或顾客关系技术栈的天然补充。由此，任何想要了解顾客群的详细特点的电子商务商家都可以与分析提供商建立一个智能的合同来创造所需的功能。尽管生态系统没有明确支持合同签订与投标的过程，但任何开发者或组织都可通过 引入新的活动类型和相关的投标与协商机制来创造这种可能性。

技术解决方案细节

主要的BASE组建

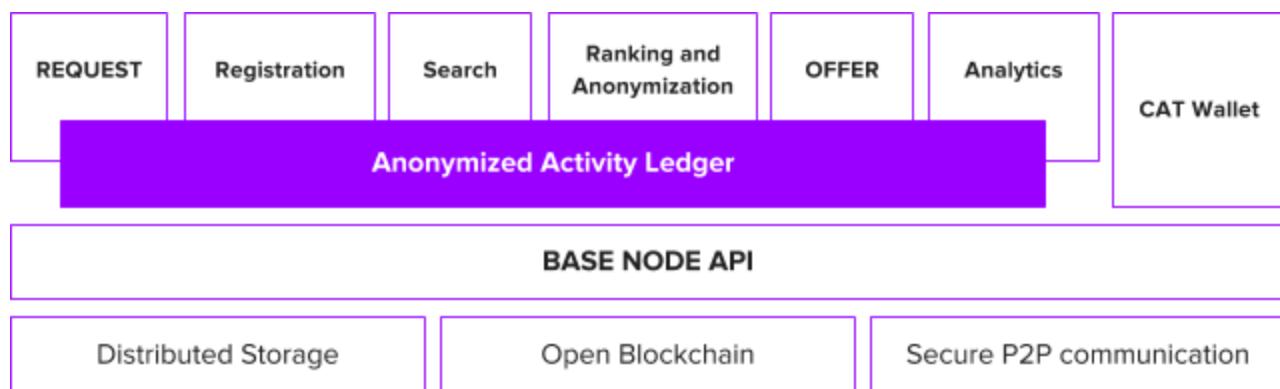


图 7:组成活动账本的多样化 BASE 组件是建立于区块链，链下存储和保密通信的基础之上的。BASE 的 API 提供了一层抽象层来减轻发展负担和支持关于具体的区块链实现的灵活程度。

注册子系统

与 BASE 的互动从注册过程开始。每一个 BASE 的参与者都需要经历这个过程。因为 BASE 是一个去中心化的系统，我们需要制定计划去阻止恶意用户利用这个系统。我们希望避免的基本情形包括了用户通过向商家报告虚假个人信息，从而获得更好的 OFFERs 或者试图多次开户以及通过多次搜索获得报酬。以上只是小部分我们需要重视并解决的流氓方案。

注册服务应当尽可能负责核实顾客/商家信息。注册服务是 BASE 中的一个独立注册实体。注册服务会通过其公钥进行识别，所以每一位权益相关的参与者可以核实注册服务 签署信息的真实性，但是只有注册服务能够创建这种签名。用户将会决定使用哪些注册服务以及哪些信息可以进行公开验证。BitClave 将会实现一个注册系统，但是如果需要的话，其他感兴趣的团体可以实现其它备选版本。

一旦用户在 BASE 中注册了，在得到用户允许之后，注册服务会核实其有能力核实的 用户提供的个人信息(或者部分个人信息)。被核实过的个人信息会经由注册服务签署并将在被商家用于提供 OFFERs 的过程中具有更高的价值。例如，如果对用户的工资信息和 当前所使用的汽车进行核实，那么在生成个性化报价时，它将给予汽车经销商更多的信心。用户总是可以选择在与系统建立更舒适的关系后再对个人信息进行验证。在注册完成后，用户的个人信息会以加密形式被存储区块链中。没人可以理解整个过程，但是用户将能够根据选择提供密钥给当事人，所以这些当事人可以解密个人信息并且可以检查这些信息是否被任意一个注册服务签署及核实过。

REQUEST 子系统

当用户与 BASE 交互时，这些用户主要是与 REQUEST 子系统进行交互。在这里，用户可以提交搜索作为 REQUEST 行为，接收 OFFERs 表单，与 OFFERs 交互从而接收观看奖励并完成销售转账。

REQUEST 子系统代表了顾客的利益。在去中心化系统中，我们有多个实体用于搜索 和多个商家对顾客的 REQUESTs 作出响应。REQUEST 子系统的主要作用就是保护用户利益以及最大化 BASE 的价值。

一些 REQUEST 子系统的重要角色包括了：

- 过滤掉不符合顾客要求的垃圾邮件或 OFFERs。这可能因为错误或者一些恶意发件 人的蓄意张贴引起
- 过滤掉不值得信任的商家，例如低排名的商家或者没有确认注册状态的商家
- 根据顾客选择的标准对多个搜索引擎的结果进行优先处理。虽然这种优化可以在顾客的 UI 层中实现，但在合同层中的实现对其他实体时可见的，并且会进一步提高 商家提供最佳匹配订单的能力
- 收集相关的个人信息是 REQUEST 过程的一部分。例如，当寻找汽车保险时，该系统可能会询问一个更详细的问题，如目前的住房保险，以前的汽车保险或人寿保险。虽然这些问题在最初的注册阶段就会引起关注，但在保险搜索询问的情形下，顾客会更容易回答这些问题。当然，顾客也可以不提供这些信息，并且他仍然会收到报价，但这些报价可能不如提供更详细的个人信息的情况好。一旦这些额外的个人信息被提供用于搜索，它们会被以一种加密的形式安全的存储在顾客账户的区块链中，之后经过顾客的同意，会被用于其它 REQUESTs 过程。
- 向顾客建议提供哪些个人信息会获得更好的 OFFER。通常情况下，OFFER 会包括 基于顾客个人信息的不同奖励(这就是针对性/个性化的报价的全部意义)。当 REQUEST 子系统收到报价时，它可以识别什么样的个人信息会给顾客带来更好的回报，并建议顾客将该信息提供给报价。顾客接下来会基于额外的奖励，和对提议的业务和其他标准的信任程度来决定是否公开其个人信息。
- 通过与 R&A 服务交互来协助顾客对他的 REQUESTs 选择最佳的匿名方式。在我们 经过基于多种匿名化方式的讨论，现在 REQUEST 子系统代表了顾客的利益，能够 为具体的转账给出最合适的方式的建议。

OFFER 子系统

当商家与 BASE 交互时，它们主要是与 OFFER 子系统进行交互。商家可以向 BASE 提交 OFFERs，基于顾客个人信息定义 OFFER 的结构，进行数据分析从而了解 OFFERs 在进行的工作以及其它相关的活动。
OFFER 子系统代表了商家利益，并且和上述 REQUEST 子系统有很多相似之处，唯一的区别就是 OFFER 面向商家而不是面向顾客。
OFFER 子系统最重要的作用包括了：



识别骗子或不值得信赖的顾客，类似在 REQUEST 子系统中一样，但更注重保护商家利益。



基于特定顾客的个人信息、顾客排名和顾客搜索请求，准备针对性 OFFERS。这也很类似于 REQUEST 子系统，但是方向“相反”并且更注重保护商家利益。



在向顾客发送奖励之前，核实“proof-of-view”报告。点击欺诈是网上广告的一个主要问题。在通过匿名化方案处理顾客的隐私问题时，我们需要解决的关键问题是 BASE 如何预防阻止恶意用户或者脚本带来的点击欺诈。相当一部分解决方案在市场上可以获得，并且 BitClave 将会选取一个现成和专有的解决方案组合来保护商家的利益。

搜索服务

搜索服务是一个将 REQUEST 和 OFFER 相匹配的独立实体。搜索服务奖励是为了使 BASE 中的交易数量得到最大化。搜索服务可以被 CATs 成功交易有选择性的激励。BASE 可以使用各种不同的搜索服务，其中一些试图优化客户体验而另一些则试图最大化商业价值。我们不想对搜索服务施加任何严格的限制，而是允许生态系统中存在竞争，客户和商业利益则分别由 REQUEST 和 OFFER 子系统保护。搜索服务可以非常专业，专注于当地服务，如水管工，保姆，学校导师，汽车，律师，财务顾问等。BASE 旨在支持系统中所有服务的实施。

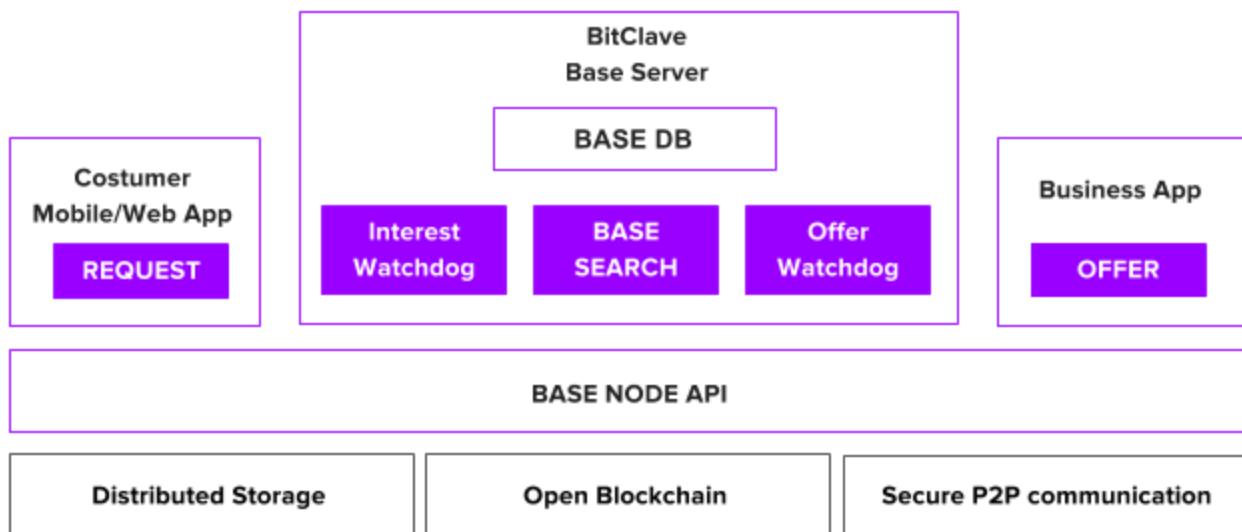


图 8:BASE 架构表明了不同服务在客户，商家和基于块链的分类帐之间发挥的交互作用。

综上所述，搜索服务在 BASE 中的作用是为 REQUEST 或 OFFER 有关潜在匹配的智能合同提供一个“recommendation”。用户最终会做出一个业务交易决定，该决定由智能合同在链上促成。搜索服务的作用相当于房地产业务中的房地产经纪人的角色。房地产经纪人将汇集潜在的买卖双方，但商户交易的最终决定仍然是由个人做出的。

以下是有关实施 BASE 搜索服务的一些细节。要实现 BASE，BitClave 承担两个角色：



一个角色是构建一个开放，去中心化的平台，实现客户和商家的直接互动，而不需要类似于第三方广告网络中的中介。



另一个是执行将此平台带给用户所需的所有应用程序和服务。

BitClave 的目标是建立一个没有中间媒介的平台。这意味着 BitClave 致力于定义一个开放的平台，因此它的安装使用将仅使用所有人可获得的信息。这种透明度保证了 BitClave 本身不是起着和广告中间人相同的作用。此外，BitClave 会为搜索和其他部分提供开源软件。

BitClave 的第一个功能是将存储关于客户，业务，提供的产品和服务的匿名信息，将所有可用的链接存储和脱机开放，去中心化的储存在一起。

BitClave 的第二个功能则是将使用脱机实体来实现高效搜索。这些实体包括从开放存储(以只读方式)检索信息的外部服务器，并将填充针对搜索进行了优化的 BitClave 数据库。当新的搜索请求进入该区块链时，BASE 将使用其数据库来查找匹配的供应商，并在区块链上将这些供应商与智能合同相连接。交易的最终决定是由用户完成的，并且是由智能合同促成。通过以上可以看出，搜索服务仅仅只是提供建议。

需要注意的是没有什么可以阻止任何其他的利益相关方实施一个更有效的基于区块链的搜索服务。由于其开源特性，BASE 只会从更好的搜索服务执行中受益，并且随着 BitClave 的用户和合伙人的持续参与，区块链技术的不断进步，推荐引擎技术将进步，这也会提升生态系统的整体性能。

排名和匿名服务

分布式和匿名系统中的排名是一个具有挑战性的课题。一方面，客户可能想要匿名，所以他们可能会在 BASE 中为不同的活动使用不同的假名。另一方面，商家希望向客户提供和他们兴趣更相近的 OFFERS，但为了建立排名，需要将多个不同客户假名的活动(包括搜索，购买和个人资料详细信息)相关联。为了讨论我们的方法，我们使用与身份，匿名，假名和可链接性相关的各种术语，这些术语符合 ISO / IEC 15408 信息技术安全评估

标准中的通用标准⁵。

在高水平上，为了保持 BASE 生态系统的开放性，我们计划为用户创建各种选择，以便他们自己在匿名和搜索价值之间进行权衡。接下来我们将描述我们打算如何解决客户不愿透露姓名与商家对可链接性的需求之间的冲突。

按客户 ID 排序

在交易的时候，客户可以通过在所有 BASE 交易中使用其主要的区块链钱包身份来完全实现匿名。在这种最简单的模式中，所有客户的信息(无论是公共的还是受保护的)都与其在分类帐中的真实身份相关联，因此其余任何人都可以对客户的搜索和采购历史进行各类分析，例如计算购买与供应的比率(即转换率)。这种模式的缺点是客户的所有历史交易活动都可以联系在一起。但是一些客户可能会选择这种最大化搜索价值的方法(但仍然保护个别交易细节)，其他客户可能会因为泄露过多他们的交易历史信息而感到不舒服。

即使具有完全的可链接性，我们也希望保护个别交易中涉及的客户数据，并有选择地向商家披露信息。为了实现这一功能，我们可以列出加密的客户数据以及搜索查询，其中每个列表项都使用没有其他人知道的对称密钥进行加密。这是所谓的加密承诺的一个例子，因为它不显示任何信息，而是将每条信息与搜索绑定。例如，此列表可能包含如下值

$$E_{k1}(info_1), E_{k2}(info_2), \dots, E_{kn}(info_n),$$

其中 E_k 表示具有对称密钥 k 的加密，并且使用不同的密钥 k_i 来加密每条信息 $info_i$ 。如果客户之后想要向零售商披露特定的信息，例如他的采购历史或某些统计资料，则可以将相应的密钥 k_i 安全地传送给商家，从而允许他们解密相关数据。举一个传送方式的例子，客户可以将经加密的消息 $EPK_j(k_i)$ 发送到公司 j ，其中 EPK_j 表示使用公司公钥 PK_j 的非对称加密。这个操作(简称开放承诺)允许零售商访问客户的私人信息，但不改变任何过去的承诺，因为块链阻止修改过去的数据。此操作(简称开放承诺)允许零售商访问客户的私人信息，而不改变任何过去的承诺，因为块链会阻止修改过去的数据。

⁵ 信息技术安全评估的通用标准，第三部分：安全确认部分 v. 3.1, rev. 4, 9. 2012,
<https://www.commoncriteriaportal.org/files/ccfiles/ccpart3v3.1r4.pdf>.

以顾客发起的假名排序

向更加强有力的匿名更进一步，顾客可以选择为 BASE 中不同的活动使用假名，由此，活动便不会被链接在一起。这样在保护顾客搜索历史的同时，还隐藏了有用的商家信息。在一些情况下，顾客可能想要向某商家显示特定链接，比如为了促成上述的一些使用案例。这可以用来证明这样的情况：一位顾客购买一辆新车后，现在需要保险，或者做其它回头生意，比如每几个月购买一双运动鞋。理想上，顾客可以向选中的商家显示特定链接，并不暴露(i)全部交易记录，或(ii)意外交易的链接。顾客是否暴露链接也取决于商家是否确实向顾客提供附加值做为信息，这是由于商家不直接向数据进行支付，但这是另一个问题。

为了理解我们如何在 BASE 中实现选择性的可链接性，回想一下，对假名最严格的使用可能意味着每个发布到账本的活动都像是来自各个独一无二的用户，意味着完美地掩盖了顾客的真实身份。在一个稍微更加实用的方法中，设想一位顾客在不同的搜索活动中使用不同的假名，比如使用假名 IDshoes 每过几周搜索新运动鞋。然而，现在假设这位顾客想展示一些 public profile 中的信息，这需要对应 profile，将假名 IDshoes 链接到顾客的真实身份 IDreal。有很多方法可以做到这样，由先前信息片段可以被加密并用于搜索的例子开始。尤其是当假名 IDshoes 被用于搜索时，顾客可以加入一个被加密的标签 $E_k(\text{sig}_{SKreal}(k))$ ，这是一个用对应真实身份的 secret key SKreal 加密的签名。没有 key 的情况下，这个加密标签是无意义的，这是由于没有 key k 的情况下，加密签名既不能被读取，也不能生效。由于在之前的案例中，顾客可以安全地向选中交易暴露 key k，从而允许交易来解锁签名 $\text{sig}_{SKreal}(k)$ ，并检验其签名为正确的 secret key 所签，由此来验证假名与真实身份之间的链接。同样地，如果顾客想将多个假名链接在一起(例如当顾客使用不同假名进行每一个鞋子搜索时)，可以共享交易列表和相应的 key 来将它们链接在一起，并使其他人不知道这个列表的存在。另外，可以在不链接顾客真实身份的情况下，将链接在假名之间完成，只需要证明这些搜索源自同一位顾客。

然而，这种使用假名而不是真实身份的交易中，可能的情况是，身份信息比其他种类的信息更加敏感，所以我们可能要提供更加强有力的保障。事实上，像上述这样使用加密签名，有一个潜在弊端，那就是它不绑定到假名，而只绑定真实身份。为了代替像我们对其它顾客信息做的那样承诺身份使用对称加密，我们建立一个更加强力的加密承诺，它以一个被检验的方法，同时绑定了假名和真实身份。做为替代，我们可以创立一个签名对，它使用非对称私/密钥 SKshoes 和 SKreal，来证明顾客同时持有这两个身份。使用假名 IDshoes，时将 signature pair 包含进搜索，可以做一个可行的方法。

$$S = [\text{sig}_{SKshoes}(k), \text{sig}_{SKreal}(k)]$$

使用随机值 k 做为每个 secret key 的签名函数中的输入。过后，当顾客想向另一参与者证明自己持有 IDshoes 和 IDreal 两个身份时，它可以相对应特定搜索来安全地共享 k 值，而其他参与者可以使用顾客的两个公钥 PKshoes 和 PKreal 使 S 中的两个签名都生效。

第三方参与者排名与匿名服务

平衡排名和匿名矛盾的另一方法是利用系统中的附加服务提供者。这个排名与匿名 (R&A) 服务有效地结合了来上述方法的益处，并促进了顾客与商家之间的私人和匿名的预约交易。使用 R&A 服务，顾客向 R&A 服务发布加密交易，它会代表顾客发布交易，并同时做顾客身份下的私人记录。R&A 服务可以读取顾客的全部交易，并可以为顾客计算真实的全球排名。R&A 服务可以在每次发布交易时使用新的假名，并附上真实顾客排名做为交易的一部分。R&A 的特殊成就是通过使用第三方参与者服务的协助，结合了上述技术。

从商家的角度上看，当交易通过 R&A 服务时，交易变得更值得信任。作为激励顾客使用次模式的方式，对比商家为匿名顾客工作时，它会为商家提供更高的自信度。顾客可以决定使用哪一种 R&A 服务。提供“有用的”排名性能可以作为对 R&A 服务的激励，它可以为它的服务收取 CAT 费用。

综上所述，顾客和商家有很多选择来控制他们的私人信息和个别活动历史。像这样，他们可以选择和决定最适合自己的方式。因为 BASE 是一个开放而有竞争性的市场，它最终会在匿名度、信任度、报酬最适合于社会时达到一个平衡点。

活动分析

如所讨论的那样，匿名活动账本的主要价值是能够共享匿名顾客和零售商数据，以帮助生态系统中的顾客和零售商提供价值的分析。分析子系统与 R&A 子系统紧密相关。它与顾客和商家之间的交流需要通过账本，以便关联交易，但其目标是向感兴趣的各方提供更全球化的观点，以便这些策略能够得到优化。

具体例子包括：

- 访问 BUY 活动的某些细节可用于分析购买趋势，识别高需求物品或公开类似模式。同样地，除了公开地发布这样的细节，还可以使用适当的密钥管理，加密的搜索或其它技术加密地控制访问。
- 顾客资料分析，个性化 OFFERs 和 BUY/非 BUY 交易活动将使商家能够为某些顾客提供奖励方面的获奖策略。
- 除了针对机会识别和预测的活动分析之外，各方可以使用活动账本中的数据来验证索赔(类似于法医证据)，例如，使用账本中的数据以满足与另一方在生态系统的智能合约的条款。

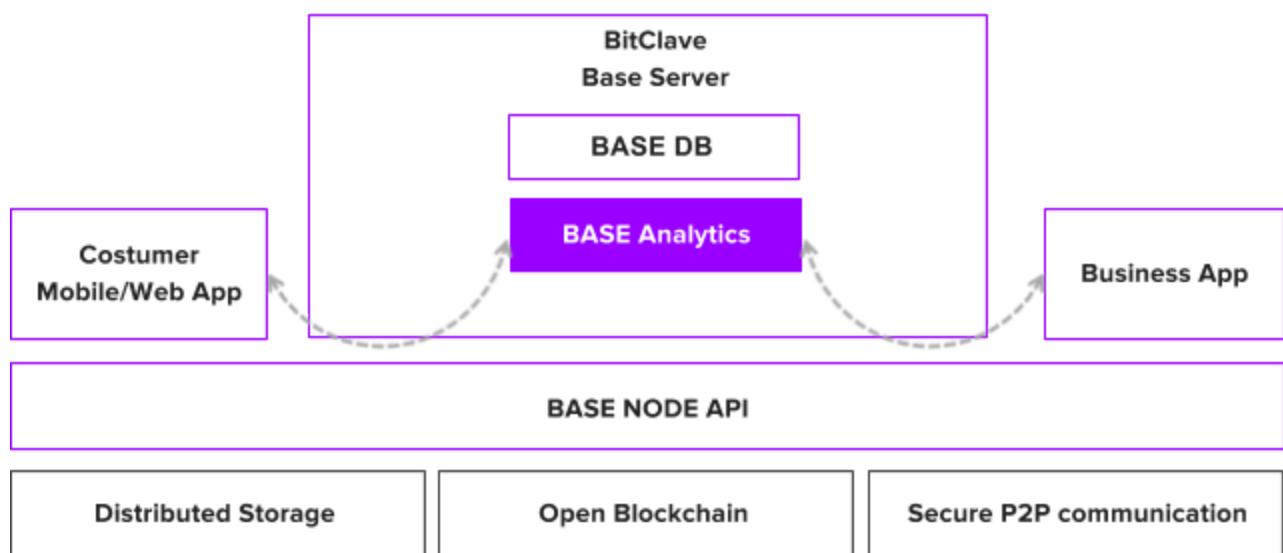


图 9:分析在 BASE 中发挥重要作用，为顾客和商家提供有关市场活动历史的数据。

分析子系统的功能取决于顾客和商家使用的匿名级别。为了说明这些变化，我们提供了一些不同分析强度的代表性例子，作为匿名级别的函数。

案例 1(匿名)

如果顾客使用独特的假名发布所有搜索，对应于最强的匿名级别，则不可能计算顾客任何类型的搜索历史，因为每个身份只使用一次。在这种情况下，商家了解顾客搜索或购买历史的唯一方法就是要求他们透露更多信息，这些信息可能依赖于能为顾客提供一些附加值的智能合同。

案例 2(可链接性)

如果顾客愿意透露其购买历史之间的联系，但不愿意透露其身份或个人资料信息，分析提供商将能够将顾客的购买历史与特定的预测模型相匹配，建议顾客可能感兴趣的其他商品和服务，例如，如果顾客将汽车修理服务和人身伤害律师服务联系起来，即使不了解顾客或其任何人口统计信息，分析提供商依然可能会建议汽车保险或医疗服务的促销活动。

案例 3(个人资料分析)

如果除了可链接性之外，顾客愿意从他们的个人资料中披露一些个人信息，分析服务可以进一步提高为顾客建议的促销的质量或价值，为顾客和潜在的服务提供商之间提供更强的匹配或更好的促销折扣。

基于营销平台分析的固有价值，BitClave 计划与开源或商业分析平台进行整合。

BitClave 维护活动账本的只限读取快照的情况显著减轻了与可用解决方案的集成。这是与 BitClave 搜索方法所看到的外部快照类似的优点。但是我们注意到，分析子系统是BASE 设想的高级服务之一，因此 BitClave 将在开发阶段的后期提供。由于 BASE 是一个开放式平台，其他供应商可以实施替代竞争的分析服务。

BASE 可扩展性和 BASE 节点 API

BASE 的愿景是建立一个完全去中心化，基于区块链的搜索平台，在此平台，用户和商家可以直接联系，而这意味着利用来自用户和商家双方的大量的数据。区块链的创新速度是非常快的，虽然像比特币和以太坊这样当前领先的区块链都认识到可扩展性的挑战，

并且为其区块链寻求解决方案，但新的平台在理论上更优化- EOS⁶, NEO⁷, QTUM⁸ 就是可提供优化交易速度的几个平台。创新发生在许多领域，不仅 是可扩展性-优化的匿名，如 ZCASH⁹ 和 MONERO¹⁰（门罗币），更安全的合约语言，如 量子链（QTUM）， 分布式存储系统，如 Filecoin¹¹ 和 SiaCoin¹²，侧面渠道解决之道，如 Raiden Networks¹³ or 最近 Plasma¹⁴ 公告。为了应付这种高创新速度，并且充分利用已有的 新的解决方案，BitClave正推出BASEAPI 层，旨在将抽象基础架构服务进行分布式计算，通信和储存。BitClave 的主要重点是开发 BASE 平台和应用/服务，以此将平台推广给用户。这就是 BitClave 带来的价值。BitClave 将在创新浪潮中发挥作用，并利用可用或成熟 的新科技。BASE NODE API 将有助于使此次发展更为顺利。

以太坊区块链

BitClave 将使用以太坊作为初始版本的平台。以太坊是一个经过验证的区块链，可提供 BASE 所需的服务。凭借强大的路线图，以太坊的能力和功能将不断改进。Metropolis¹⁵ 通过 zkSNARKS¹⁶ 和 Serenity¹⁷ 改进的匿名性，在近距离功能和等离子体中具有‘工作 证明’和‘股权证明’仅仅是几个例子，以显示以太坊是一个非常有吸引力的平台。

为了说明这些以太坊改进的价值，BASE 将提供以下没有任何优化的使用以太坊区块 链的 BitClave 搜索的例子，然后再展示每种补充技术可以如何提供附加值。

作为开始，让我们假设 BASE DB 有很多 OFFERs.在步骤 1 中,客户提交有关于区块链的 搜索请求。BitClave 搜索(Search)会检测到已经提交的新请求(步骤 2)。接下来它会在 BASE DB 里去搜索相对应的促销(步骤 3)并将建议的匹配项交给区块链给 OFFER 合约来 考虑这个提议。OFFER 会阅读新的提议(步骤 4)，对推荐执行内部验证来确保 Search 的 推荐符合搜索要求，并且开始沟通原始的 REQUEST 合约(步骤 5)。作为步骤 5 的一部分，OFFER 会提议给 REQUEST, REQUEST 会验证这个提议符合要求(提示， REQUEST/OFFER/SEARCH 互相之间都不信任)。REQUEST 会把促销呈现给用户，用户可 选择查看促销与否，如果这个促销被查阅了，查阅证明就会被回执给 OFFER 来得取奖励。为了简化这幅图表，我们将步骤 5 中所有有关于 REQUEST 和 OFFER 之间的沟通步骤总结 在一个双向箭头中。

⁶ <https://eos.io/> -分权应用最强大的基础设施

⁷ <https://neo.org> -分布式智能经济网络

⁸ <https://qtum.org/en/> - 区块链为商业做好了准备

⁹ <https://z.cash/> - Zcash是第一个开放的，无权限的加密机制，可以使用零知识加密技术充分保护交易的隐私

¹⁰ <https://getmonero.org/> - Monero（门罗币）是一种安全，私密，不可追踪的货币

¹¹ <https://ipfs.io/> -一种对等的超媒体协议，使网络更快，更安全，更开放

¹² <http://sia.tech/> - Sia在分散的网络中分离，加密和分发文件

¹³ <http://raiden.network/> -高效资产转让给以太坊

¹⁴ <http://plasma.io/> - Plasma: 可扩展自主智能合约

¹⁵ V. Buterin, “Ethereum R&D Roundup: Valentine's Day Edition”, Feb 2017, <https://blog.ethereum.org/2017/02/14/ethereum-rnd-roundup-valentines-day-edition>

¹⁶ C. Reitwiessner, “zkSNARKs in a nutshell”, Dec 2016, <https://blog.ethereum.org/2016/12/05/zksnarks-in-a-nutshell>

¹⁷ V. Buterin, “Understanding Serenity, Part I: Abstraction”, Dec 2016, <https://blog.ethereum.org/2015/12/24/understanding-serenity-part-i-abstraction>

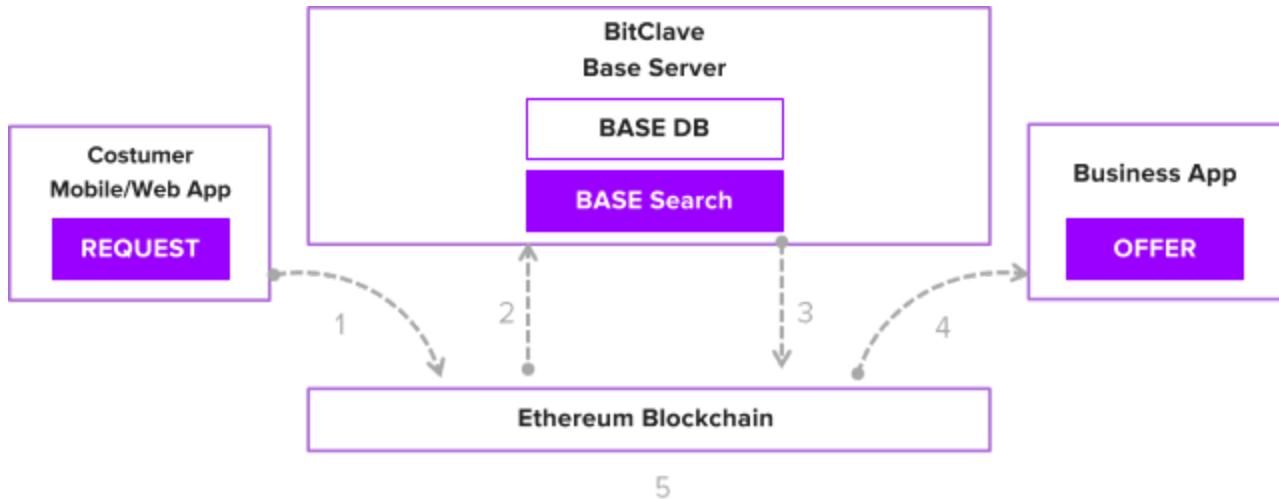


图 10:用以太坊来说明基础搜索活动的活动流程。

储存的可伸缩性

以太坊提供了一个用于去中心化储存的设备。遗憾的是，如今以太坊提供的解决方案偏昂贵。在区块链内储存信息，需要支付 20000GAS 仅仅用于单指令储存 32 字节的数据，使用平均 4gwei 的 GAS 价格是大概 0.02 美元。这样按比例计算，那些预期要通过 BASE 平台的交易，单单 GAS 的费用就能达到数百万美元。

BitClave 正在寻找更好的解决方案来有效的降低费用和提升性能。如今已有多种解决方案，同时 BitClave 正在研究多方面的技术。PFS¹⁸/Filecoin¹⁹, Storj²⁰, 和 SiaCoin²¹ 是目前团队正在评估的一些技术。

¹⁸ <https://ipfs.io/> -一种对等的超媒体协议，使网络更快，更安全，更开放

¹⁹ <https://filecoin.io/> - Filecoin：分散存储网络

²⁰ <https://storj.io/> - 基于区块链的端到端加密分布式对象存储，只有您可以访问您的数据

²¹ <http://sia.tech/> -你的分散的私有云

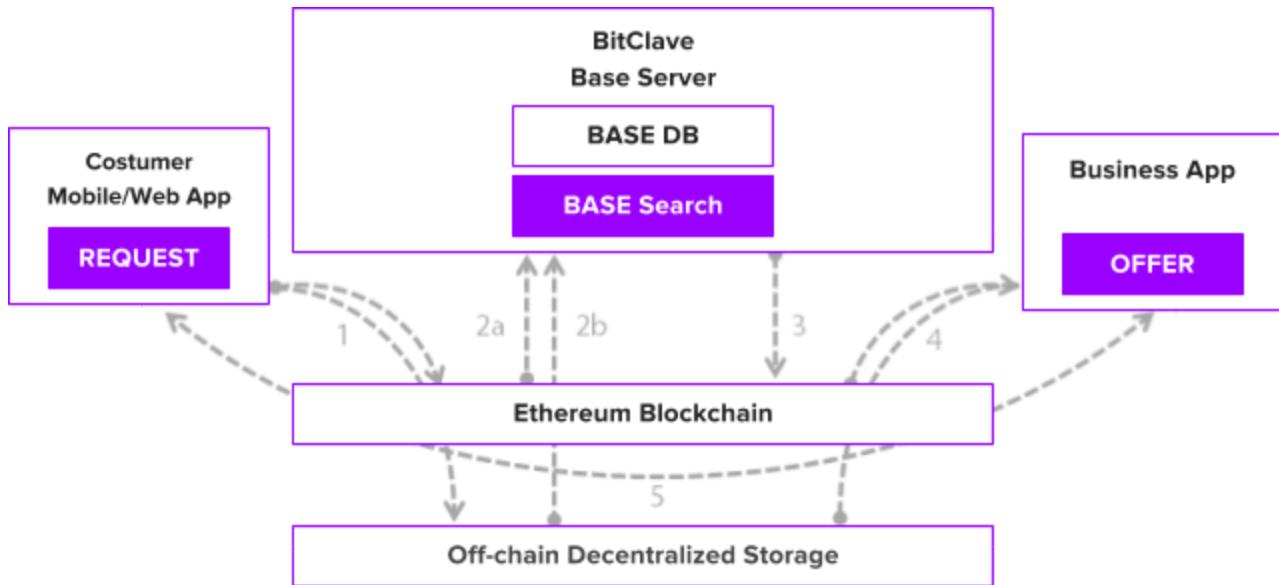


图 11: 使用区块链外的去中心化储存连同以太坊一起，将会减少发布在以太坊上数据的规模，从而降低 GAS 的费用以换取和公共储存系统的通讯。

为了充分利用“区块链外的去中心化存储”，我们将会做如下的修改：当 REQUEST 写给区块链，现在就只有单一指示会被写入区块链，而其余的数据将会被写入公共外部储存器。因此，BASE 搜索将必须遵循来自区块链的指示，从而访问到来自外部储存器的完整 REQUEST 细节。OFFERS 也将遵循类似的体制。

交易速度

以太坊的交易速度是每秒钟几十次(参阅近期的 CoinTelegraph 通告²²来获得更准确的数据)。在不久的将来，随着越来越多的 DAPPS 被应用到以太坊，并在 BASE 上产生大量的交易，交易速度将有可能会成为一个问题。为了降低风险，BitClave 会使用与 Raiden Network²³ or Bitcoin Lightning²⁴ 使用相类似的技术，来部署安全的 P2P 频道。

²² W. Suberg, “Ethereum Breaks Blockchain Transaction Record, Price Steady”, The CoinTelegraph, Aug 2017, <https://cointelegraph.com/news/ethereum-breaks-blockchain-transaction-record-price-steady>.

²³ <http://raiden.network/> -高效资产转让给以太坊

²⁴ <https://lightning.network/> -可扩展的即时比特币/区块链交易

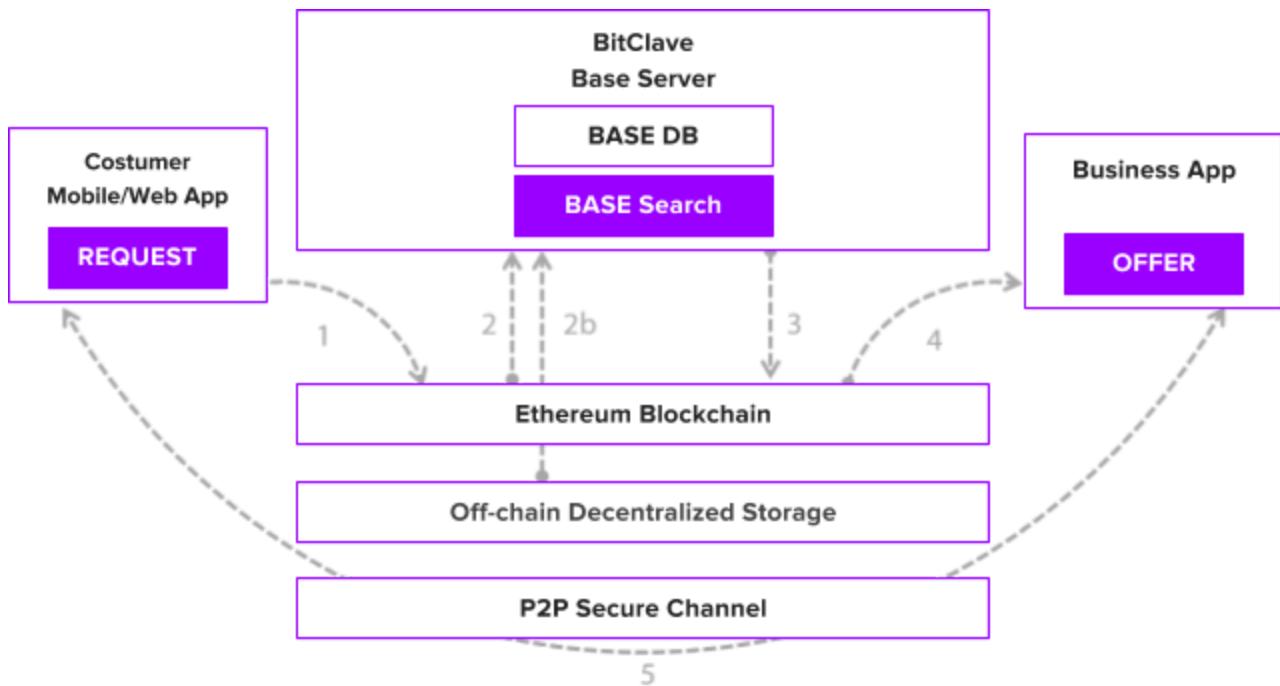


图 12:直接的 P2P 安全通信可以运用于进一步从区块链中分流一些 BASE 的互动，从而提高被以太坊 所限制的性能和速度

正如第四步所描述的，所有的沟通都在 REQUEST 和 OFFER 之间，而区块链的剩余部分并不关心这次协商的细节。重要的是交易是否发生，所以我们可以为步骤 5 使用一个直接的“状态通道”，并且只写出最后的结果给区块链。此外，如果 OFFER 来自一个客户会持续购买的商家，那么这个状态将会储存在区块链外更长的时间，直到其中一方决定将状态发布到区块链以供分享。在此情况下，更多的交易将会从主区块链中分流出去。

法律

BitClave在新加坡成立了BitClave私营有限责任公司(BitClave Pte. Ltd.)，而BitClave公司(BitClave Inc.)的总部和运营地位于美国加利福尼亚州。BitClave总部、创始人及很多开发团队成员都在美国，并遵守和执行当地联邦、州和地方相关法律的所有要求。为了确保整个BitClave项目和公司结构符合法律要求，BitClave与 Schiff Hardin和Cooley等知名律师事务所建立了合作伙伴关系。

此外，我们还增加了几位重要的区块链顾问，如Bancor的Guy Benartzi，TenX的Chris Miess，Gambit Capital的Sten Laureyssens，以及ICON的Min Kim。他们不仅在如何成功运营区块链新公司、建设BASE等方面给予我们支持，还帮助我们借鉴行业优良传统，确保ICO的合法实施。

发展计划

综上所述，BitClave 活动搜索生态系统是一个创造用户驱动和激励零售机会的平台。

作为平台的提供者，BitClave 的主要关注点是建立生态系统的中心框架，所有开发者 都可以在此创建应用程序和服务。从某种意义上，BitClave 和 Facebook 用法类似，只是一个零售生态系统，一个是社交网络。因此，BitClave 支持 B2C 生态系统(以及 B2B 技术支持)的核心产品将包括核心应用程序(基于浏览器和应用程序)以及 APIs，数据库和 SDKs,这些都允许外来开发者在平台上创建(类似于 Facebook Graph API)。在另一方面，为提供一个没有既定中介商的开放平台，BitClave 以生态系统内任何第三方开发者 相同的方式，提供类似服务以及衍生收入。BitClave 应用程序受益于先发优势，以及与生态系统服务提供者的紧密结合，但是在—个去中心化的平台上，开发者和服务提供者 “out BitClave” BitClave 是合情合理的。

此外，BitClave与Bancor合作，在BitClave 活跃搜索生态系统（BASE）上已使用智能代币。BitClave已加入 Bancor 网络，并将成为其协议族的成员。顾客活动代币（CAT）将使用ERC-20代币标准，与所有交易所兼容，并与Bancor网络上的其余货币将能交易。

同样令人激动的是，BitClave还与QTUM建立了合作伙伴关系。Qtum是一个混合型的区块链应用平台。Qtum的核心技术结合了比特币核心的优势，允许包括以太坊虚拟机（EVM）在内的多种虚拟机的帐户抽象层，以及旨在解决行业用例问题的权益证明共识。BitClave主动搜索生态引擎（BASE）这样的企业级区块链应用之所以选择Qtum，是因为它使用权益证明作为共识机制。网络使用者越多，交易量越高，达成真正共识所需的能量就越多。区块链通过权益证明，有机会提高处理交易吞吐量的能力，因此受到企业和BASE这类活跃度高的生态系统的青睐。

初期发展投入

平台的初始设计将会基于前述的请求(REQUEST)和促销(OFFER)的活动。我们设想一个具有“搜索引擎”界面的移动应用程序(作为用户的认证点(AP))，来允许用户通过 发起对特定的服务或产品的搜索请求来创建请求(REQUEST)活动。符合用户兴趣请求的 零售商和服务提供商可以提交促销(OFFER)给客户，并且通过给他们适当的支付奖励来 激励他们查看和/或者回应给 OFFER.我们也将实施 VIEW 活动来支持“查阅证明”和从商家支付 CAT 代币给客户来查看促销(OFFER)。

至于进一步的活动创造功能，例如浏览在线零售商，以及启动与零售商或者其他用户的交易(即创建 BUY 和 SELL 活动)，我们将逐渐包括进移动应用程序中。

2017年10月中旬，产品的alpha版本已经完成。该alpha版本目前正在内部测试，并将于2017年10月底，在 ICO开始之前公开发布。正式产品将于2018年发布。

早期平台用户的价值和经验

虽然生态系统的真正价值将需要时间来实现，达到足够数量的零售贡献者和用户参与者，但我们认为零售平台的早期采用者有足够的价值。从一开始，该平台将支持对等合同，这将为零售市场的引导提供价值。

平台推出后，BitClave团队将把重点放在市场营销上，以打造中小企业零售市场，预计更多的零售商将带来更多的客户，导致生态系统的持续增长。

发展计划

作为初始生态系统引导的一部分，我们已经引进了 15-20 个小型公司作为 BASE 市场 的初始实例。我们的团队将继续瞄准那些为个体用户市场营销投入大量精力的行业，例如 汽车销售，房地产，酒店，和像 Target 这样的零售商，这些和亚马逊这样的主流广告服务 提供商展开竞争的行业。一旦我们的小市场建立起来，我们将会增强我们的营销力来不断

扩大参与者的数量。

新机会

BitClave 设计和开发一个开放资源的去中心化搜索生态系统，外来开发者可在系统中 创建应用程序和服务。核心产品包括允许外来开发者在平台上构建的框架。

代币分配

ERC-20代币将在销售结束后4周内发行。

筹款计划

到目前为止，我们已经成功完成了代币预售活动。11月29号开始全面开放众筹。筹款活动将继续进行，直至达到2500万美元的硬上限（或60天）。正式开始日期将通过官方BitClave渠道宣布。在fundraiser.bitclave.com上注册关于筹款活动的最新公告。

交易所

BitClave与许多交易所合作，以确保二级市场上的代币及时上市。

用户利益

用户将按照上面规定的初始兑换率得到对应的 CATs 数额。既然 CATs 的总量是固定的，那么在持续增长的零售合作伙伴和客户之间，代币的交换就表明 CAT 价值的普遍增长模式。特别是随着越来越多零售商和客户加入 BitClave 生态系统，贡献给活动账本的活动数据的数量和质量也将逐步提高，也就是说每个数据贡献的奖励将减少。同样的，当越来越多的服务提供者加入时，在同类 CAT 价值增长的情况下，对于同等服务所需要的 CATs 数量也会逐渐减少。总体而言，以服务提供者的最低运营成本和最低额度的参与者激励金额为基础，我们预计 CAT 的市场价值将稳定下来。

团队

BitClave 成立于 2016 年，其愿景是重新定位基于智能合约的信任和透明度智商的客户 和商家之间的关系。我们的解决方案有可能破坏世界上最大的市场之一，由巨头商家垄断，由中间商操控的广告网络市场。

世界各地的人民与政府都对个人隐私的保密性感到担忧。而这种担忧大都归功于隐私侵 入式数据挖掘实践中的'免费服务'的诱饵调包手法的模式。

这些做法对于他们所声称支持的商业经济是合理的，但却导致连续性的脱节促销和购买， 商家为了与直接销售几乎没有关联的指标付出了高昂的代价，同时从质量，忠诚度和价值建设中转移了大量重要的资源。

我们致力于使用去中心化和开放的方式参与市场，以提高当地经济的服务质量和社 会责 任感。

对于 BitClave 来说，如果隐藏的广告网络能被转化升级为一个活动驱动市场，世界将会 更加美好。在这个市 场中，顾客和品牌可以共享价值创造红利，同时培养有意义的关系，搭 建起买卖双方的桥梁。

执行团队

团队由 20 位工程师和一个顾问委员会组成。委员会拥有在安全、支付、区块链领域世界级 的人才。



CEO, Alex Bessonov

超过 20 年安全、隐私和区块链行业高管经验。前 LGE 首席安全官。



CTO, Patrick Tague

卡耐基梅陇大学电子与计算机工程系研究副教授。移动、嵌入式和无线安全方面专家。



首席架构师, Emmanuel Owusu

卡耐基梅陇大学博士。安全、区块链、物联网、公共政策和隐私方面专家。



项目管理, Vasily Trofimchuk

CS 硕士, MBA。连续创业者, 擅长博奕论、区块链、管理。



区块链开发者, Anton Bukov

斯坦福大学硕士学位，企业家，加密学，电信与计算机科学专家。计算机系统专家，软件数据安全和私有处理。区块链爱好者和开发者。



高级开发人员, Ivan Yurin

引导后端开发人员，具有可扩展系统的经验。



核心开发者, Andrey Shashlov

专注于 Android 和 iOS 的全栈开发人员。商家家和创业者。区块链爱好者。



数据架构师 , Eugene Kaganovich

资深 Java 全栈开发者。商家云数据保护专家。



数据科学家, Mark Shwartzman

特拉维夫大学硕士学位。视频压缩和数据科学专家。比特币爱好者和开发者。

专家顾问

Expert Advisors



区块链顾问, Min Kim

ICON基金会的联合创始人。 DAYLI金融集团首席战略官。 DAYLI风险投资合伙人。



战略顾问, Alex Shin

Blockchain Partners Korea的合伙人。 TeamBlind产品运营主管, 用户采购/增长。



区块链顾问, Greg Wolfson

企业家和区块链专家。 前BTCC业务发展总监



区块链顾问, Lucas Hendren

伊利诺伊大学明矾电气与电子工程双学士和物理学硕士。 区块链企业家和专家。
SimplyVital Health联合创始人。



法律顾问, Doug Park

博士斯坦福GSB, JD密歇根州。 在公司治理, 商业模式, 监管策略和组织领域专家。



管理顾问, Gerald Beuchelt

LogMeIn中的CISO。 Demandware前CISO。 Infragard成员联盟波士顿分会董事会成员。



战略顾问, Kevin Doerr

微软, 雅虎, Weather.com和GoDaddy高管。 在用户体验, 安全和团队建设领域的专家。 天使投资人。



数据安全顾问, **Balaji Ganesan**

连续创业者。 Privacera首席执行官。 数据隐私和安全方面的专家。 专注于GDPR合规性。



战略顾问, **Enrico Ferro**

马里奥·博埃拉研究所（ISMB）创新发展部主管。 米兰理工大学博士学位。



法律顾问, **Reza Dibadj**

哈佛JD和MBA。 擅长解决商业法和商业策略中的复杂问题。



科学顾问, **Brad Gaynor**

塔夫茨大学电子工程博士学位。 Lexumo的创始人和首席技术官，在德雷珀实验室建立网络系统业务。



战略顾问, Elie Galam

Eastmore集团首席投资官。 哈佛大学应用数学硕士。

术语表

活动

一种在 BASE 上能被匿名活动账本记录的行为。这种活动包括网上行为(例如, 搜索请求, 查看个性化订单, 网上购物)以及线下行为(例如, 访问零售店或购买产品)。这种活动可以与顾客, 商家, 或两者同时有关(参照活动定义)。

匿名活动账本

使用匿名化和不可链接技术的相关顾客和零售商活动的去中心化账户(见 匿名活动账本)。

BitClave 活跃搜索生态系统

指代定义去中心化认证平台以及行为数据搜索的一整套协议 系统(也被引为活跃搜索或去中心化搜索。 见 BASE 定义)。

顾客活动代币(CAT)

参与各方在所有交易中使用的代币。这些代币为零售活动市场中的 各种服务提供奖励(见 代币驱动基础)。

零售分析提供商

一个提供分析能力服务的实体 (见 零售分析提供商).

可选择性链接性/不可链接性

基于团体的访问控制可以被用于控制哪一方能够链接活动到 一个普通(即使有可能是未知的)身份(见 基于团体的活动共享)

智能合约

一个在生态系统里, 双方或多间, 自动执行的合同。它将一组活动映射为待 执行的账本操作。

代币兑换

一个由社区建立的兑换率，给某特定活动或服务赋予了价值。(见 用来激励参 与的代币)。

关注我们吧！

<http://www.bitclave.com/>



info@bitclave.com



<https://github.com/bitclave>



<https://twitter.com/bitclave>



<https://www.facebook.com/bitclave>



<https://linkedin.com/company-beta/6399312/>



<https://slack.bitclave.com>



<https://t.me/BitClaveCommunity>



<https://www.youtube.com/channel/UCtibs4mNHqbPn-NGnFtK6yg>



<https://bitcointalk.org/index.php?topic=2005370>