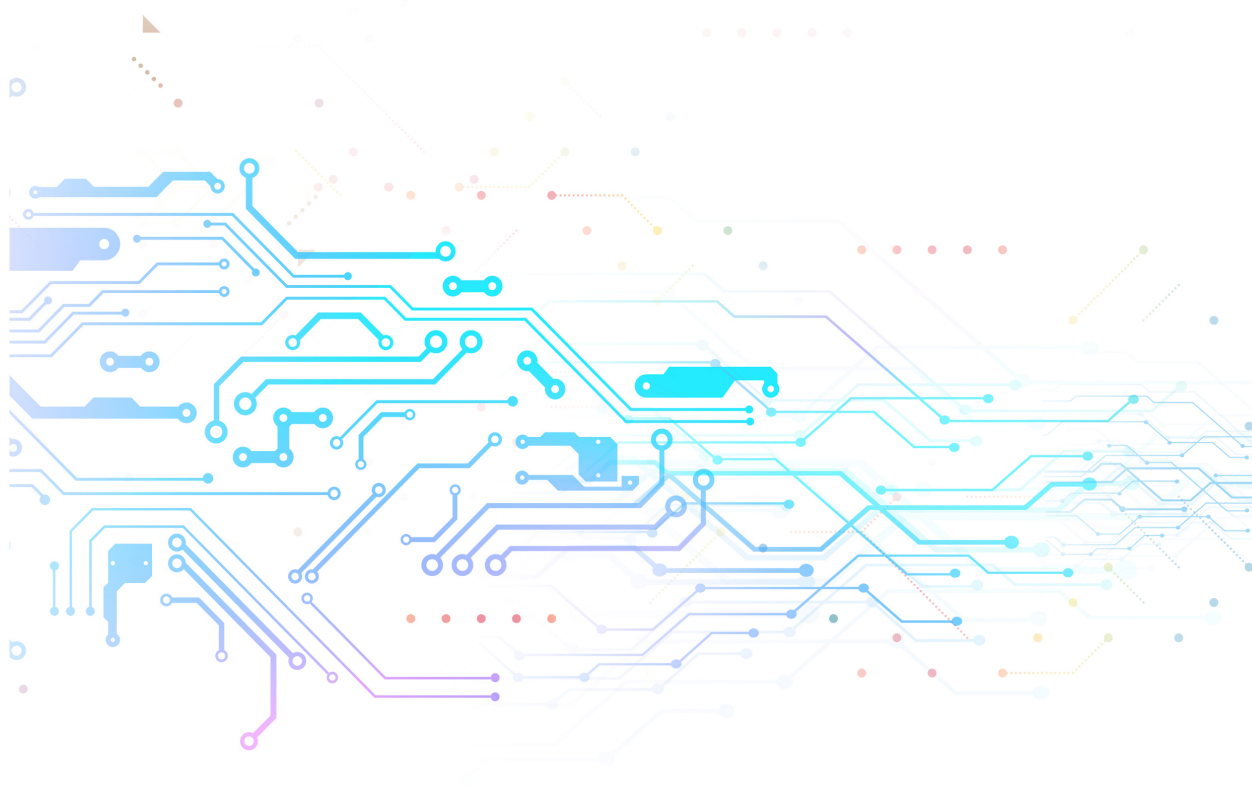




百度区块链白皮书V1.0



发布：百度搜索公司 百度区块链实验室 百度营销研究院

时间：2018年9月

蜜蜂内参

让您深入洞察整个商业世界

每天精挑细选3份最值得关注的学习资料

关注公众号：**mifengMBA**

回复“入群”加入“蜜蜂内参”城市群

(不需要转发哦.....)



扫一扫
回复“入群”

序 言

当今世界，信息技术革命日新月异，对国际经济、文化、社会、军事等领域的发展产生了深刻影响，“数字化、网络化、智能化”深入发展，在推动经济社会发展、促进国家治理体系和治理能力现代化、满足人民日益增长的美好生活需要方面发挥着越来越重要的作用。

互联网改变了信息传递的方式，人工智能释放了计算能力，从重复、低效和繁重的工作中把人解放出来。区块链基于其分布式、防篡改、可追溯等特点构建的新型信任机制，将加速生产价值的“数字化”流通，改变价值的传递方式。区块链的开源性、可编程、去中心等特性，将进一步打破信息孤岛，扩展“网络化”运行的边界。机器流程引擎驱动多中心跨主体高效协作，社会资源将实现共商共识共享共治的“智能化”配置，带给区块链应用前景的无限憧憬和想象。

目前全球正在掀起一股基于区块链技术的创新热潮。各国抢占未来前沿领域技术优势的力度之大，国际竞争之复杂和激烈是空前的。区块链技术带动经济 and 产业格局的重大调整，将是中国实现跨越式发展，在国际分工中占据有力地位的重大转折机遇。2016 年 12 月，区块链首次被作为战略性前沿技术写入《“十三五”国家信息化规划》。2017 年 1 月，工信部发布《软件和信息技术服务业发展规划(2016-2020 年)》，提出区块链等领域创新达到国际先进水平等要求。2017 年 8 月，国务院发布《关于进一步扩大和升级信息消费持续释放内需潜力的指导意见》，提出开展基于区块链、人工智能等新技术的试点应用。截至 2018 年 3 月底，我国以区块链业务为主营业务的区块链公司数量已经达到了 456 家，产业初具规模，进入高速发展阶段。

百度作为中国在尖端科学核心技术领头的高科技企业，秉承“用科技让复杂的世界更简单”的使命，积极配合国家战略层面的指引方针，以公平开放、技术赋能、生态联盟为准则，致力于构建行业区块链应用生态，将区块链的价值赋能给包括政府、企业及个人用户的社会各个层面，为降成本、提效率、优化产业诚信环境、价值重新分配等方面贡献力量。百度区块链实验室，全面布局区块链生态的各个领域，包括 XuperChain 底层基础设施建设，企业级的解决方案 BaaS (Blockchain-As-A-Service)，以及服务于创造数字经济和改善社会生活的一系列区块链应用等。

百度将在数字技术创新、安全可控、自主研发等方面持续推动区块链的社会价值和经济价值，建设“网络强国、数字中国、智慧社会”，为我国产业结构迈向全球价值链中高端，实现经济高质量发展贡献力量。

（1） 网络强国，中国速度

信息化为中华民族带来了千载难逢的机遇，互联网经济以数据为关键生产要素，通过运用网络信息技术提升全要素生产率和优化经济结构。区块链是继云计算、大数据、人工智能之后的又一新兴网络信息技术，其基于技术构建的信任机制，基于合约和规则达成的多节点共识，基于机器驱动的价值自动化流通，将极大的改变当前社会的商业模式，进而引发新一轮的技术创新和产业变革，为数字经济带来新的活力。

百度运用领先的区块链技术驱动数字经济创新，推动互联网和实体经济深度融合，加快传统产业数字化和智能化，催生出更多新产业、新业态和新模式，用新动能持续升级新经济发展。

（2） 数字中国，自主研发

2018 年注定是不平凡的年代，在日趋复杂的国际合作与竞争中，核心技术受制于人是我们最大的隐患。互联网核心技术包括：核心芯片、人工智能、量子计算、区块链等。

百度区块链秉持自主研发，打造关键核心技术上的独有优势：运用超级节点无限扩容区块链的计算和存储能力，彻底突破区块链的性能瓶颈，独创立体网络技术（包括：链内 DAG 并行技术、可回归侧链技术和平行链技术），充分利用超级节点所提供的可伸缩性存储计算，采用可插拔共识技术以满足业务方多样性需求，通用智能合约运行机制兼容区块链开发者生态和程序员开发生态，并从底层机制上保证了在合理的规则框架下实现自我升级和自我修复。

核心技术是国之重器，要下定决心、保持恒心、找准重心，加速推动信息领域核心技术突破。百度积极响应习近平主席对于自主创新的期望：努力实现关键核心技术自主可控，把创新主动权、发展主动权牢牢掌握在自己手中。

（3） 安全可控，健康发展

没有网络安全就没有国家安全，就没有经济社会稳定运行，广大人民群众利益也难以得到保障。网络安全已经进入国家战略。安全是数字经济创新的基础，没有安全一切将无从谈起。

百度区块链拥有自主知识产权，研发与迭代不会受到恶意势力组织的干扰。百度区块链秉持安全可控的健康发展理念，坚决反对侵犯个人隐私、侵害知识产权等各类网络违法犯罪行为。

百度区块链自身具备的技术和特性保证数据隐私、价值流转和网络治理的安全可控。百度区块链将运用 SHA256、RSA、非对称椭圆曲线、抗量子等加密算法，以及零知识证明算法、安全多方计算等技术组合，保障数据隐私的安全，防止数据泄漏。

与此同时，百度区块链运用加密和共识算法构建的信任机制，将推动建立安全可信的数字经济规则和秩序，保证价值流过程的安全可控，促进不同国家、不同地区、不同经营单位和不同个体间开展更加紧密的数字经济合作。从而保障，在安全可控的前提下，促进网络安全和信息化事业的健康发展。

（4） 智慧社会，链聚天下

网络安全和信息化事业发展必须贯彻以人民为中心的发展思想，区块链创新应用 DApp (Decentralized Applications)，将适应人民期待和需求，加快信息化服务普及，降低应用成本，为老百姓提供用得上、用得起、用得好的信息服务，让亿万人民在共享互联网发展成果上有更多获得感。

百度带头推进“区块链+传统产业”升级、“区块链+教育”、“区块链+金融”、“区块链+文化”、“区块链+知识产权”等领域的 DApp 开发，充分发挥全链路共享共治，让数据多跑路、百姓少跑腿，不断提升公共服务均等化、普惠化、便捷化水平。

发展网络安全和信息化事业需要人才，百度区块链作为开放式平台技术，将提供一站式、全赋能、即插即用的区块链系统，汇聚世界水平的科学家、网络科技领军人才、卓越工程师、高水平创新团队，施展商业价值和社会效益的才智，打造“取智于人才，造福于人民”的共创共享共荣的中国区块链生态。

是以为序。

百度搜索公司

百度区块链实验室

百度营销研究院

2018 年 8 月 16 日

编委会成员

顾问：向海龙、梁志祥、吴海锋、郑子斌、尹世明

指导专家：林晓东、侯丽斌、马杰、陈志峰、王建勇、丁宗尧、王岳

执行主编：谭待、肖伟

统稿：裴玖、刘虎、高苗、杨天依、高倩、李王浠

研究撰写：卞琦、柴桥子、陈浩栋、董淑照、段兵、范围、高倩、顾庆立、
顾晓莉、侯迪、黄心远、荆博、李王浠、李元嵩、刘国庆、刘虎、
刘强、刘尧、刘志伟、龙丽莉、宋飞、宋利华、孙健、孙君意、
谭待、唐涛、王冠薇、王辉、王磊、卫晓霞、肖伟、闫石、于雅楠、
张晋豪、张伟、张岩、郑旗、周辰、朱延峰

法律顾问：邓凯

市场及公关：李姝、孙瑜

视觉设计：田丰玉、黄海伦

目 录

第一章 区块链发展概述.....	1
1.1 区块链概念	1
1.2 区块链价值	1
1.3 区块链发展现状	2
1.3.1 公有链与联盟链	2
1.3.2 DApp 生态	3
第二章 百度区块链整体架构.....	4
2.1 区块链行业痛点	4
2.1.1 当前区块链技术的性能制约	4
2.1.2 智能合约的痛点	4
2.1.3 共识机制的痛点	5
2.1.4 计算和存储的痛点	5
2.1.5 网络建设的痛点	5
2.2 XuperChain 网络介绍	6
2.2.1 运行结构	6
2.2.2 共识机制	6
2.2.3 超级节点	7
2.2.4 智能合约	8
2.2.5 立体网络技术	9
2.2.6 轻量级节点技术	11
2.2.7 可升级系统	11
2.2.8 隐私保护和安全	12
2.3 XuperChain 网络生态和基础设施	13
2.3.1 网络生态	13
2.3.2 超级链 App	13

2.4	结语	14
第三章	百度区块链商业化解决方案	15
3.1	百度区块链商业化介绍	15
3.1.1	区块链即服务 BaaS 的现状和需求	15
3.1.2	区块链商业落地的问题及应对	15
3.1.3	百度区块链商业化布局	16
3.1.4	百度云区块链的产品和技术框架	17
3.2	百度区块链行业落地案例	21
3.2.1	金融区块链场景案例	22
3.2.2	物联网区块链场景案例	23
3.3	百度云区块链的发展规划	23
第四章	百度区块链行业应用	25
4.1	内容版权	25
4.1.1	内容版权领域的发展趋势	25
4.1.2	内容版权领域的痛点	25
4.1.3	内容版权的区块链解决方案	26
4.1.4	内容版权未来的发展规划	28
4.2	信息溯源	28
4.2.1	互联网信息领域的痛点	28
4.2.2	百度百科在信息溯源的区块链解决方案	29
4.2.3	百度百科未来的发展规划	31
4.3	文化娱乐	32
4.3.1	文娱产业现状	32
4.3.2	度宇宙的产品定位	33
4.3.3	度宇宙解决方案	33
4.3.4	度宇宙未来的发展规划	36
4.4	信息安全	36

4.4.1	反恶意软件行业的痛点	36
4.4.2	反恶意软件区块链解决方案（休伯特）	37
4.4.3	休伯特未来的发展规划	38
4.5	个体信息管理	39
4.5.1	个体教育信息管理领域的痛点	39
4.5.2	个人教育信息的区块链解决方案（百度会学）	39
4.5.3	百度会学区块链的实现路径	42
4.5.4	百度会学未来的发展规划	44
4.6	数字广告	44
4.6.1	数字广告领域的问题及应对	44
4.6.2	通用搜索广告的区块链解决方案（百宝箱）	46
4.6.3	百宝箱未来的发展规划	47
未来与展望		48

第一章 区块链发展概述

1.1 区块链概念

区块链起源于比特币，是一种综合技术的简称。在经历了多年发展后，不断集成当今多种技术于一体，包括分布式账本、共识机制、智能合约、密码学、P2P 网络等。在每个区块链系统中，区块即信息块，信息以区块的形式进行集成、打包，并按照实际产生时间的先后顺序进行连接。

1.2 区块链价值

如今，伴随诸多区块链项目的兴起与发展，人们不断见证着区块链为各领域带来的变化，也逐渐认可区块链技术本身所呈现出的价值。其价值主要体现在以下几个方面：

- (1) 安全：基于去中心化 P2P 网络技术，区块链系统中所有参与节点将共同完成数据的存储、维护，可有效避免中心化数据系统遭到攻击时数据泄露的风险。在数据传输过程中，密码学技术提供了安全保障。此外，新区块的产生，是由全网多数节点达成共识后的结果，任意节点都无法实现数据的完全控制，保证区块信息不可篡改；
- (2) 确权：区块链的另一个价值体现在数据资产所有权的确认上。数据一经上链，即可通过区块链网络确定与用户间的锚定关系，且后续的每一次数据操作都会被准确记录，不可篡改。该特点可对数据资产进行有效保护，防止他人恶意篡改、窃取与利用；
- (3) 信任：去中心化区块链系统中，数据账本存于各节点，信息公开透明，为数据可信提供了基础保证。由于采用共识机制，各节点需要按照严格的算法规则更新区块信息，从而达成信息共享、多方决策一致，保障数据记录过程的可信性。整个过程中，无需借助第三方机构即可建立信任网络，完成多节点的可信沟通；
- (4) 自动化：智能合约是一种可编程化的数字协议，当合约参与方满足触发条件后，合约条款将自动执行。智能合约的加入，为区块链带来了新的契机，保障部署在区块链上的合同条款可以实现自动、去中心化的计算，从而为诸多领域（尤其针对流程复杂繁琐、效率低下的领域）的效率提升、成本控制起到不可忽视的作用；

- (5) 价值共享：传统中心化系统常涉及较多环节，参与中介多、流程复杂，耗费成本较高。而区块链系统则实现了各参与节点的去中心化连接，且各节点数据资产可进行点对点自由流通，以降低中间成本。此部分节约成本将以收益的形式，根据对区块链网络的贡献程度按照一定规则分配到各节点，在激励其他节点积极参与的同时，实现全网价值的再分配。

1.3 区块链发展现状

区块链生态构成主要包括区块链网络、基础设施（如资产管理、轻量级节点、交易所）以及运行在区块链网络中的 DApp。自 2009 年比特币网络成功运行以来，区块链各类技术得到了突飞猛进的发展。尤其是底层技术，自 2017-2018 年至今发展势头明显。基于底层平台，各领域不断进行商业端、用户端的场景落地尝试，DApp 应用持续推陈出新。

1.3.1 公有链与联盟链

区块链平台根据去中心化程度、应用场景的不同，可划分为三类：公有链、联盟链、私有链。不同区块链平台在准入机制、共识算法等诸多方面均存在差异。

公有链常被形象化为“区块链世界的操作系统”，此类区块链平台允许节点自由加入网络，且所有节点均有权查看账本信息。典型的、当前应用最为广泛的公有链平台为以太坊。以太坊提供了图灵完备的编程语言，允许开发者部署智能合约，可帮助处理复杂业务流程。然而，受限于交易处理速度、可扩展性等，以上公链平台难以进行大规模商业应用落地。自 2017 年以来，区块链逐步成为能够构建更高效社会活动的一种社会关系，成为能够减少摩擦提高效率的新范式。业界开始追求公链底层技术新的突破，探索更加普适、稳定的公链平台，并将基于该类平台的下一个时代定义为区块链 3.0。目前，公链 3.0 平台仍处于探索阶段，大部分主网暂未上线。据各平台对外公布数据，可以预见的是，2018 年将是公链 3.0 平台高速发展的元年，各公链主网将陆续于 2018 年下半年至 2019 年完成上线。

联盟链通常被用于政府机构、商业机构及公司之间，节点通过准入机制得到授权后方可加入，不同节点所拥有的信息查看权限不同。典型的区块链联盟项目如超级账本（Hyperledger）、R3。超级账本（Hyperledger）项目由 Linux 基金会发起，旨在构建跨行业开源区块链商业平台，推动各行业成员协同合作、共建开放平台、简化业务流程。

其中，专注于提供企业级区块链解决方案的 IBM HyperLeger（也即 Fabric）区块链平台备受关注。R3 是由美国初创公司 R3CEV 发起的金融行业区块链联盟，目前已吸引多家国内外金融机构加盟。该项目旨在为银行业提供探索区块链技术的渠道，同时开发分布式账本平台 Corda。

私有链不在本白皮书讨论范围内，此部分内容已略去。

1.3.2 DApp 生态

随着区块链（尤其是底层平台技术）的发展，各领域快速进行着区块链应用的原型设计、功能测试，直至最终产品落地。当前，以太坊平台受到诸多开发者的认可与追捧，并基于该平台持续进行技术落地创新，DApp 不断涌现。截至 2018 年 6 月，以太坊平台已有 DApp 数量超过 1600，生态最为繁荣。其中，较为知名的如世界首款区块链游戏 CryptoKitties、以太坊钱包 imToken、社交聊天应用 YeeCall 等。除以太坊外，其他底层平台也陆续衍生出了各具特色的应用生态，拥有各自典型的 DApp，如基于 Steem 平台的 Steemit、基于迅雷链的玩客云、基于公信链的公信宝等。

然而总体来看，DApp 发展仍处于初步探索时期。绝大多数 DApp 在产品设计上尚未成熟，没有充分体现出区块链技术的独特优势。在诸多 DApp 生态中，暂无可以与传统 App 相匹敌的爆款 DApp 出现，用户体量相对较低。

第二章 百度区块链整体架构

2.1 区块链行业痛点

2.1.1 当前区块链技术的性能制约

自区块链技术诞生以来，区块链的性能问题一直是倍受业界关注和讨论的核心问题，同时也可能是成为区块链行业发展的壁垒。当前，影响区块链性能的直观指标可总结为四点：

- (1) 出块时间：区块产生的时间间隔；
- (2) 区块大小：单个区块的实际存储容量；
- (3) 事务执行速度：单个请求的处理时间。对于包含智能合约的请求，执行速度还受智能合约的执行时间影响；
- (4) 事务大小：事务数据存储区块链里的实际大小。

回顾区块链 1.0 时代的比特币交易系统，性能的制约因素可归纳为区块大小和出块时间。区块链 2.0 时代的以太坊系统，由于支持通用智能合约，除了区块大小和出块时间之外，只能利用单核 CPU 的串行计算的低效率同样是制约整体性能的因素。同时，POW 机制以较慢的出块时间来降低分叉概率的机制，也是影响区块链整体性能的因素之一。

2.1.2 智能合约的痛点

以太坊的出现，让人们注意到用智能合约可以构建丰富多彩的价值网络。但以太坊本质是一个基于单链架构的通用智能合约系统，所有的智能合约都在一条链上运行。所以以太坊的合约之间没有隔离能力，性能也差强人意。除此之外，以太坊提供的 Solidity 语言设计上存在欠缺，也缺乏实用的编程库支持，无法跟主流编程语言比较。

深挖智能合约的潜力，我们认为丰富的智能合约可以完整的构建一款基于区块链的应用程序，我们叫 DApp（Decentralized App）。DApp 能够传递有价值可信的信息和服务。区别于现在的 App，现在的移动 App 提供的信息和服务需要主体公司的信用做背书，而在 DApp 中，背书是由区块链完成的，因此 DApp 比 App 具备巨大的优势。DApp 取代 App，标志着区块链技术 3.0 时代的到来。为了迎接新的时代，两个技术问题亟待解决：

- (1) DApp 运行的独立性：每个 DApp 都可以跑在一条或者多条链上，DApp 内部的智能合约相互可以访问，DApp 之间的数据通过跨链通讯来实现；
- (2) DApp 开发的便利性：智能合约的编程语言，短期内应该向当前的软件开发生态靠齐，支持主流编程语言包括 C++，JAVA，Go 等。但是从长期来看，区块链的智能合约需要有更符合自己特点的原生编程语言。

2.1.3 共识机制的痛点

共识机制本质上是一套博弈系统：共识的产生需要付出一定的代价，矿工努力工作后能获得有效的奖励，通过一奖一罚的博弈保证系统稳定实施。现存的共识机制，在应用层面比较专注于某一特定场景并存在一定程度的短板。比如 PBFT 比较适用于联盟网络的共享账本技术，POW 能耗较高、POS 存在中心恶意干涉的可能性等。

在当前的技术背景下，功能过于全面的共识算法无法真正可用。在新一代区块链共识机制的设计过程中，根据实际应用场景，有的放矢的选择去中心化、节能、安全等设计原则，对一些原则支持强弱进行取舍，将一定程度上提升系统的整体运行效率。因此，在新一代的区块链系统设计中，可插拔的共识机制可能是未来发展的主要方向：在区块链解决方案中，应该实现兼容多种共识算法，在实际业务落地中有选择性的使用一种最合适的共识机制，甚至整个网络具备让开发者自定义共识机制的能力。

2.1.4 计算和存储的痛点

在当前的区块链技术方案中，始终无法突破单机的存储和计算瓶颈，甚至连单机的多核计算和多盘存储都不能很好的利用。整体性能和扩展性存在一定局限。性能支撑是用户体验的基础，因此区块链支撑 DApp 的良好运转，必须解决计算和存储的弹性扩展问题。

2.1.5 网络建设的痛点

- (1) 平台化技术的难点

- 1) 基于比特币等公链平台实现 DApp 的难点

目前公链的技术，如比特币，如果想直接用比特币的区块链网络做自己的事情，有两种模式：

- ① 将数据写到比特币的 Script 区里面，业务端理解数据并实施；

- ② Fork 比特币的代码并进行修改，从头开始搭建自己的区块链网络。

通过这些模式创建自己的 DApp 对网络构建、技术实施的门槛非常高，一定程度上限制了 DApp 生态的快速发展。

2) 基于以太坊公链的平台化难点

基于以太坊的平台化主要面临两方面问题：

- ① Solidity 这门语言相对较弱，在构建复杂应用的时候，会面临软件工程的问题；
- ② 以太坊的整体网络性能，不足以支撑一款高频 DApp 的执行，所以根本无力去支撑整个 DApp 生态。

(2) 区块链建设的难度

公链的建设难度极大，利益纠纷明显。在传统比特币和以太坊的区块链公链建设过程中，需要大量的矿机和电力加入。而 EOS 的网络建立，需要强大的社区运营以及资源支持。如果每一个 DApp 的出现，都要自己去建设公链，对开发者来说将是一个巨大的挑战。

为解决上述痛点，百度发布 XuperChain，作为操作系统级别的区块链解决方案。

2.2 XuperChain 网络介绍

2.2.1 运行结构

XuperChain 简称超级链，是一个支持平行链和侧链的区块链网络。在 XuperChain 网络中，有一条特殊的链——Root 链。Root 链管理 XuperChain 网络的其它平行链，并提供跨链服务。其中基于 Root 链诞生的超级燃料是整个 XuperChain 网路运行消耗的燃料。Root 链有以下功能：

- (1) 创建独立的一条链；
- (2) 支持与各个链的数据交换；
- (3) 管理整个 XuperChain 网络的运行参数。

XuperChain 是一个能包容一切区块链技术的区块链网络，其平行链可以支持 XuperChain 的解决方案，也同时支持其它开源区块链网络技术方案。

2.2.2 共识机制

- (1) 可插拔共识机制

在当前的技术背景下，没有哪一种共识机制是完美无缺的，每一种共识机制都有其优点和缺点，不同的应用场景可能需要不同共识机制。为了应对不同的应用需求，XuperChain 设计了一套可插拔的共识机制，所谓可插拔主要体现在两个方面：

一方面，XuperChain 不同的平行链允许采用不同的共识机制，以此来满足不同的共识应用需求，用户可以通过 API 创建自己的区块链，并指定初始的共识机制。

另一方面，XuperChain 还支持在任意时刻通过投票表决机制实现共识的升级，从而实现共识机制的热升级。

XuperChain 的共识机制包括但不限于 POW、POS、PBFT、中心化共识（Raft）等。

（2） DPOS 共识算法创新—TDPOS 共识

基于 POS 基础上衍生出了很多改进算法，DPOS 就是其中一种。DPOS 算法是用户通过投票选出代表进行区块的生产。

XuperChain 自主研发实现了一套 DPOS 共识，我们称之为 TDPOS。依据这种算法，全网持有通证的人都可以给候选人投票。

TDPOS 的参数包括每轮的 proposer 个数、出块间隔、节点每轮出块个数等，在创建平行链的时候可以指定，也可以通过提案机制升级。通过 GPS 和原子钟保证时钟同步。例如，如果配置的参数为每轮 21 个节点、出块间隔为 3s、每个节点每轮出块个数为 200 个，则每轮的时间为 3.5h。

（3） 自定义共识机制

如果 DApp 开发者觉得系统默认的共识机制都无法满足自身的业务需求，可以通过智能合约和共识机制的编程接口，编写自己的共识，并以智能合约的形式发布到 XuperChain 中。XuperChain 在启动用户创建的这条链的时候，会注入自定义共识（需要取一个唯一名字），成为该链的共识机制。

2.2.3 超级节点

超级节点是一种分布式计算技术，保证每个节点的存储和计算是可以扩展的。从而为区块链网络提供源源不断的存储和计算支持。

（1） 存储支持

超级节点会存储所有的历史事务的完整信息，如何支撑 PB 级别的容量非常具有挑战。

XuperChain 底层 KV 存储引擎主要有以下几个特点：

- 1) 事务性表格系统：通过前缀编码的平展化，支持多链 + 多表，且能保证跨链事务的原子性；
- 2) 多盘技术：实现 KV 存储引擎到底层文件系统的虚拟映射层，支持单机多盘存储，从而支撑大容量数据存储；
- 3) 混盘技术：实现冷热数据自适应调度，将低频数据存储在 SATA 介质或者云存储，高频数据存储在 SSD 介质；
- 4) 云优化：实现 DFS 适配层，支持分布式文件系统，存储容量理论上可以扩展到 PB 级别。结合混盘调度，保证性能最优。

(2) 计算支持

在非 POW 的共识机制下，超级节点的主要计算量为交易上链和合约执行。很多区块链软件对交易的执行以及合约的执行都是串行执行的，优化到极致也只能使用单核，对硬件的利用率很低。超级节点采用多核并行计算与分布式计算相结合的方式以提升计算效率。

- 1) 多核并行计算：XuperChain 通过智能合约的依赖关系将待打包的事务构造出 N 个 DAG。每个 DAG 的交易和合约执行都是并行跑在多个 CPU 核上，DAG 内部无路径依赖的节点也可以并行执行，从而可以最大化 CPU 的利用率，突破系统吞吐瓶颈。平行链和可回归侧链技术也能有效的利用多核并发；
- 2) 分布式计算：XuperChain 未来构建事务执行的分布式调度集群，链内并行事务和多链事务可分发给调度集群执行，从而利用分布式计算的扩展能力。

2.2.4 智能合约

(1) UTXO Base 的智能合约模型

我们认为 UTXO (Unspent Transaction Output) 相对于 Account 余额模型，并发性能更好，对热门账户的性能也更优秀。超级链底层是基于 UTXO 模型，因此任何针对比特币系统的优化都适用于 XuperChain。

XuperChain 在 UTXO 的基础上做了智能合约的扩展，在扩展区可加载各种不同的合约虚拟机，每个合约机需要实现运行合约和回滚合约两个接口。回滚机制是为了应付分叉设计的，我们在合约回滚方面进行三个方面的优化，用户可以选择其中之一去实现：

- 1) 自定义回滚逻辑；
- 2) 利用区块链数据操作日志，生成反向回滚日志，自动生成回滚逻辑；

3) 引入 MPT, 分叉无需回滚支持, 但是暂时只有 KV 存储能力。

(2) 智能合约兼容

1) XuperChain 内嵌合约机制

内嵌合约机制, 规定智能合约编写的接口, 可直接用当前语言 (Go, C++, Java 等) 编写智能合约放到 XuperChain 里面。当前 XuperChain 的 Kernel API 和共识机制算法都是用这种方式实现的。

开发者可以直接写新的智能合约, 放入到 XuperChain 网络中, XuperChain 给予一定的安全隔离和保护。一般这种模式只建议联盟链部署的时候使用, 因为公开的节点会因为安全问题拒绝为该链提供算力。

未来会引入智能合约 Store 和对智能合约的安全审计, 保证发布的智能合约是安全的, 从而让公开节点放心支持。

2) 第三方兼容

XuperChain 直接支持以太坊的 Solidity 语言。以太坊的智能合约代码可以在 XuperChain 部署和执行。XuperChain 同时支持 WebAssembly, 并通过其支持任意语言。理论上 XuperChain 支持任何虚拟机的运行。

2.2.5 立体网络技术

(1) 链内并行技术

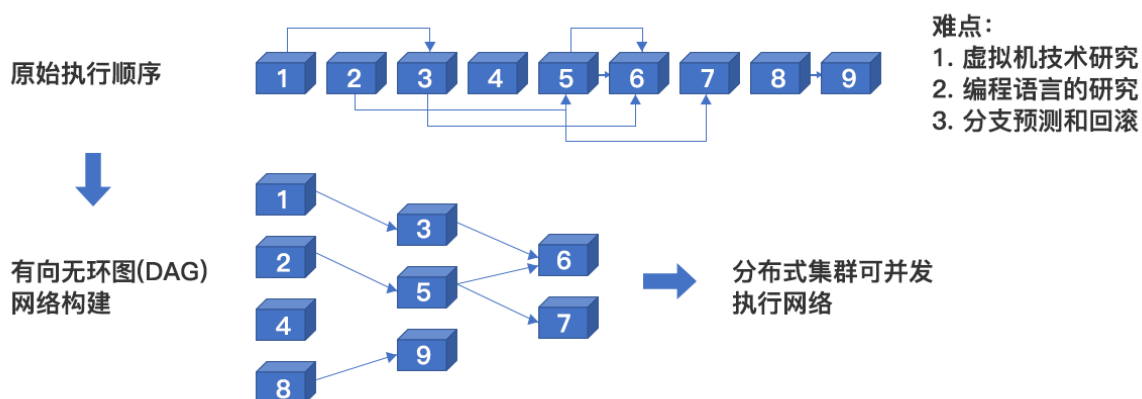


图 1 链内并行技术示意图

当下区块链技术的实现是将所有事物打包后顺序执行。随着智能合约越来越复杂, 如果顺序执行智能合约, 高并发度将难以实现, 而且也不能充分利用多核和分布式的计算能力。

为了让区块里面的智能合约能够并行执行，XuperChain 将依赖事务挖掘形成 DAG 图，并由 DAG 图来控制事务的并发执行。

(2) 可回归侧链技术

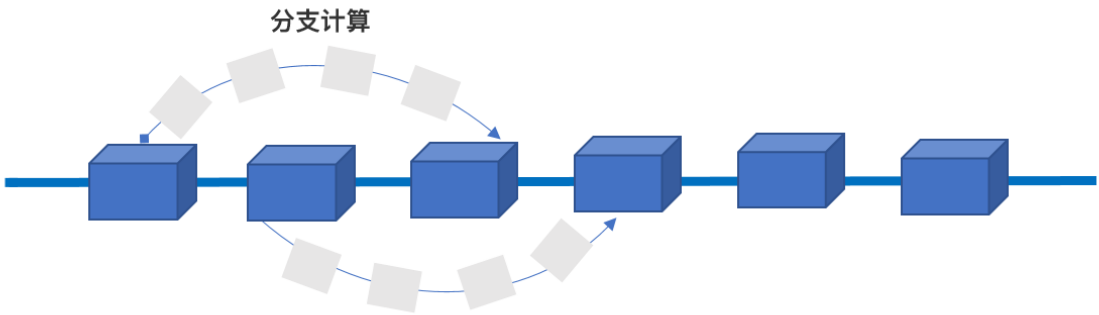


图 2 可回归侧链技术示意图

在很多场景下，并不需要把所有的事务都集中在主链上运行。比如一个运营活动，完全可以把资源放到一个侧链上去，然后通过智能合约执行逻辑，执行完成后一次性合并回主链。通过把复杂的智能合约在侧链执行，可以实现利用其它的并行计算资源去执行而不消耗主链的资源。当满足侧链回归条件的时候，主动引发侧链合并。

(3) 平行链技术

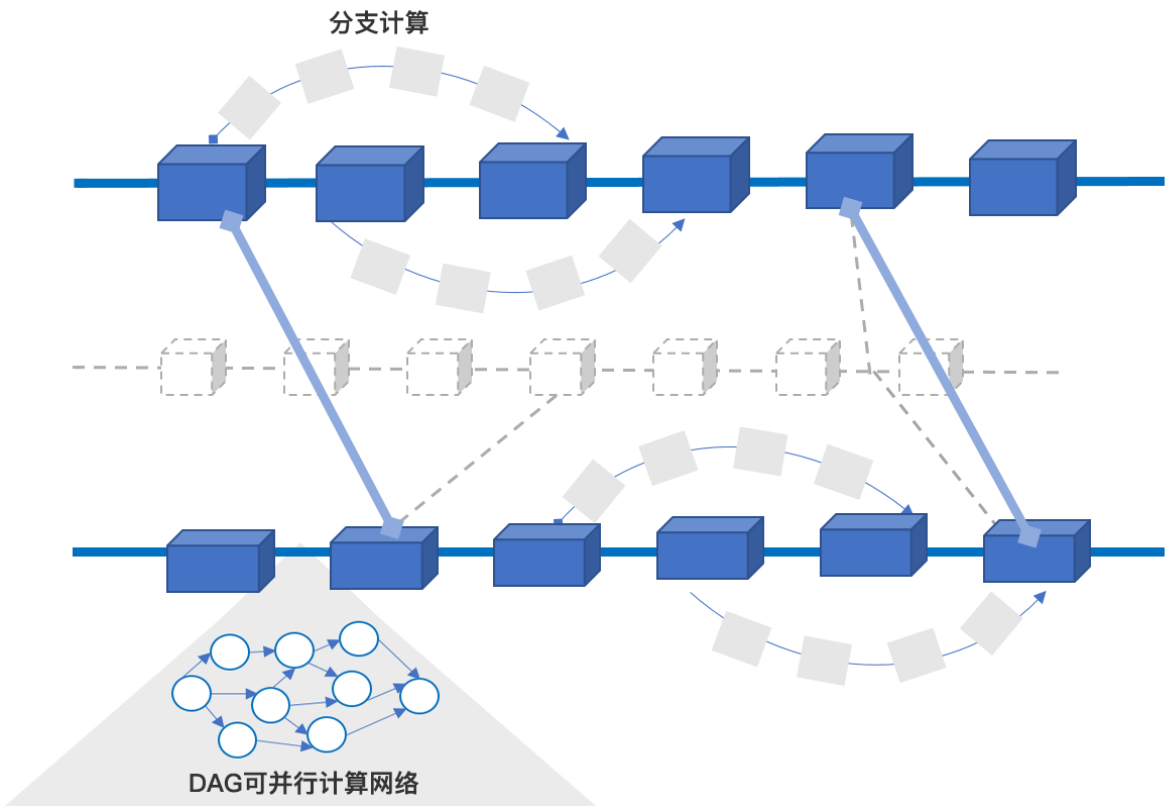


图 3 平行链技术

在 XuperChain 的立体网络里面，有大量的区块链存在。这些链通过 Root 链管理起来，这些链就是平行链，从而形成一个真实、独立存在的区块链体系。我们把这个网络叫做立体网络。立体网络上通过 Root 链创建的平行链，可以选择是公开链，也可选择是联盟链（仅成员可见）。

2.2.6 轻量级节点技术

XuperChain 在设计的时候就支持轻量级节点技术。轻节点仅同步少量数据就可以完成数据的访问和校验。轻量级客户端可以部署在 PC、手机、嵌入式设备等设备上，不需要算力和存储支撑就能有效的访问区块链网络数据。

2.2.7 可升级系统

(1) 提案和投票机制

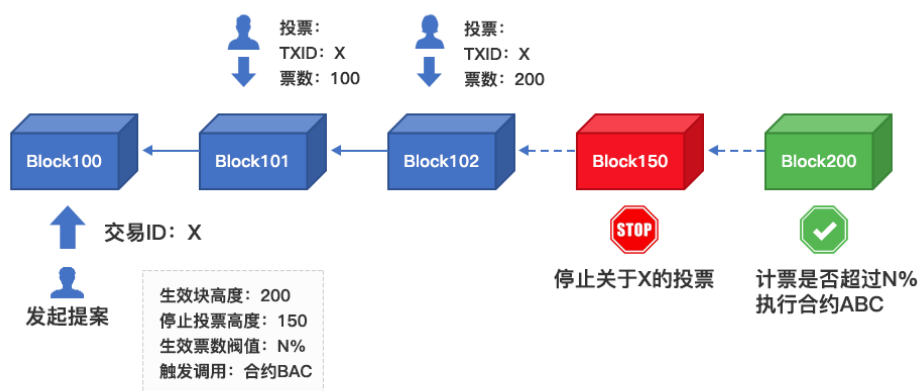


图 4 提案和投票机制示意图

提案和投票机制是区块链系统实现自我进化的关键。系统首次上线后难免遇到很多问题，我们提供提案/投票机制为区块链的社区治理提供便利的工具，以保证未来系统的可持续发展。具体实现方法如下：

Step1: 提案者 (proposer) 通过发起一个事务声明一个可调用的合约，并约定提案的投票截止高度，生效高度；

Step2: 投票者(voter) 通过发起一个事务来对提案投票，当达到系统约定的投票率并且账本达到合约的生效高度后，合约就会自动被调用；

Step3: 为了防止机制被滥用，被投票的事务需要冻结参与者的一笔燃料，直到合约生效后解冻。

(2) 共识可升级

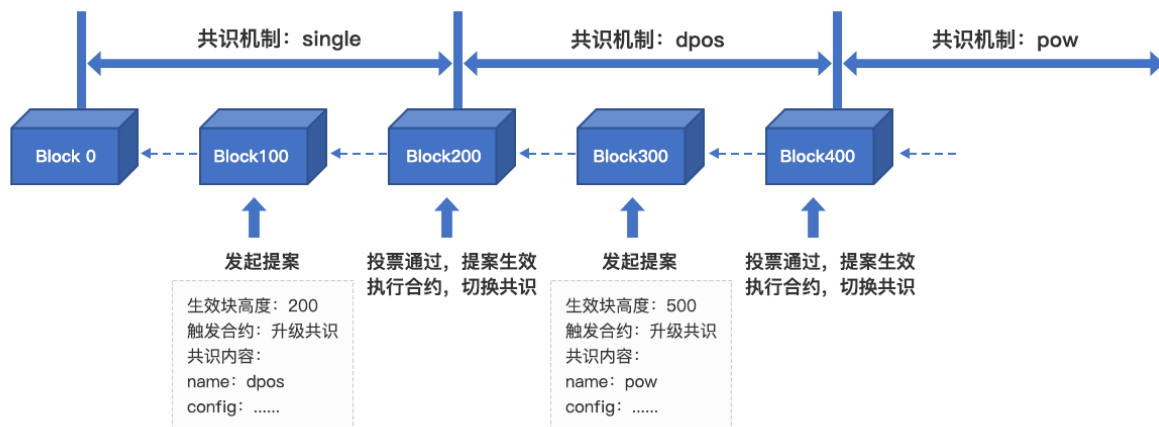


图 5 XuperChain 提案机制进行共识升级

XuperChain 提供可插拔共识机制，通过提案和投票机制，升级共识算法或者参数。

图 5 简要说明了如何使用 XuperChain 的提案机制进行共识升级。

(3) 系统参数可升级

通过提案和投票机制，区块链自身的运行参数也是可升级的。包括：block 大小、交易大小、挖矿奖励金额和衰减速度等。

2.2.8 隐私保护和安全

超级链支持多种主流的隐私保护和安全机制，包括但不限于：

- (1) 通过获取用户设备上产生的随机熵，来生成随机数种子，再通过密钥衍生推导函数来加强随机性，最后生成 ECC 的公钥私钥对；
- (2) 引入分层加密技术来降低密钥被泄露和破解的可能性。也防范了通过交易记录猜测个人隐私的可能；
- (3) 为了防止地址碰撞和输入错误，使用高强度的散列和摘要算法以及校验码来保证地址合法性；
- (4) 引入语言亲和性的助记词技术，用户只要记住助记词，就可以恢复自己的数字钱包。

2.3 XuperChain 网络生态和基础设施

2.3.1 网络生态

(1) 商业化能力

通过 XuperChain 网络创建区块链需要冻结超级燃料。

在系统稳定运行一段时间后，冻结的超级燃料会按照一定比例分给为该区块链提供资源和服务的节点。平行链持有者，为了保证区块链正常运作，应该定期补充冻结一定比例的超级燃料。Root 链是管理平行链和解决跨链的关键，Root 链的每一次 API 调用，都要消耗超级燃料。因此，超级燃料将作为 XuperChain 使用者支付使用费用的途径，也是当下 XuperChain 的主要商业化途径。

(2) 开源计划

- 1) XuperChain 已经在 Xuper 联盟内部开源；
- 2) 2019 年上半年向全社会开源。

2.3.2 超级链 App

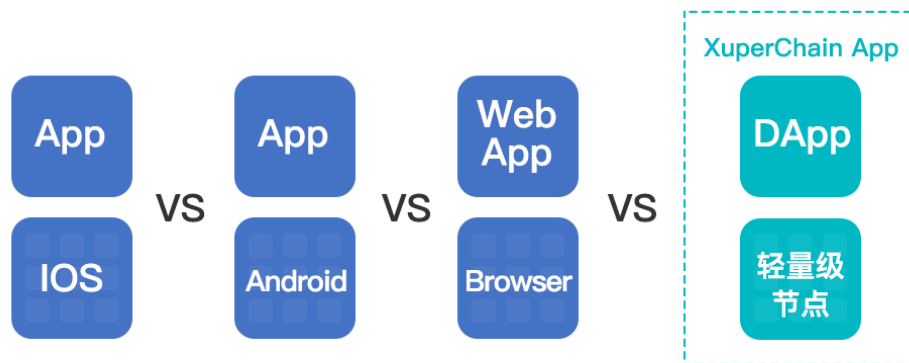


图 6 XuperChain APP

XuperChain 构建未来 DApp 运行的基础网络。一个完整的区块链生态体系需要提供一个窗口，以连接用户和区块链网络。因此推出基于百度区块链生态的超级链 App。

超级链 App 是 DApp 的终端运行平台，是用户发现并使用 DApp 的入口。开发者可以通过超级链开发者平台快速创建和发布自己的 DApp 并发行到超级链 App 中，用户无需下载即可在超级链 App 中使用所有的 DApp 提供的服务。

生态内的 DApp，可以借助百度流量优势获得流量。通过内容与服务推荐，精准的连接开发者与用户，致力于打造自治共荣的区块链分发生态服务。

基于区块链的 DApp 无法简单直连服务器，因为单独一个网络节点无法被客户端信任。所以在 XuperChain 上运行的 DApp 都是通过轻量级节点实现去中心运行。XuperChain 提供 DApp 运行的最基本的轻量级节点支持，以实现让开发者像开发 Web 程序一样开发 DApp。

2.4 结语

区块链技术作为技术迅猛发展大背景下的新兴产物，旨在通过其去中心化、开放性、自治性、防篡改性及可追溯性等特质，解决信任问题，意义重大。XuperChain 作为百度操作系统级区块链解决方案，旨在通过搭建底层生态，打造业务闭环，以赋能 DApp 开发者，使其充分拥抱区块链能力。百度 XuperChain 正以兼容并包的姿态，广纳全世界 DApp 开发者，与百度 XuperChain 一起在区块链的丰沃土壤中生根、发芽、开花、结果。

第三章 百度区块链商业化解解决方案

3.1 百度区块链商业化介绍

XuperChain 是百度自研提供的区块链操作系统技术。同时，百度也注意到在不少政府机构与企事业单位里，仍然有大量私有链和联盟链的定制化应用需求。因此，依托 XuperChain 技术为主，百度云和百度区块链实验室一起打造了一套完整的区块链商业化解解决方案。

3.1.1 区块链即服务 BaaS 的现状和需求

(1) BaaS 是区块链技术应用的赋能中心

随着人们对区块链技术的理解和挖掘，目前这项技术开始被广泛应用于支付清算、溯源、安全、媒体和出版等多个 B 端领域，基于区块链的应用也迎来了大爆炸式的发展。然而，由于区块链技术本身的技术门槛高和网络复杂度等原因，构建自己的区块链网络和应用时，往往需要付出巨大的时间和研发成本。基于此类问题，区块链即服务 BaaS(Blockchain as a Service)应运而生，其优势很明显：

- 1) 大幅降低区块链网络的研发和使用门槛；
- 2) 大幅降低区块链网络的部署和运维门槛；
- 3) 利用云计算的可伸缩性，大幅降低运营成本。

BaaS 是区块链技术的一种新型云服务，可以帮助用户快速建立属于自己的区块链网络。BaaS 结合云计算的优势后，在创建、部署、运行及监控管理等方面，体现出强大的工具属性，是区块链生态的赋能中心，同时具备私有链、联盟链等多种场景的适配能力。

3.1.2 区块链商业落地的问题及应对

经过了 2017 年的爆发式增长后，区块链行业进入平稳期，同时还未出现杀手级的技术框架和技术应用。区块链的创新发展，仍然依托于现实商业环境的实践，此过程面临诸多问题与挑战：

- 1) 标准化不统一；

- 2) 商业身份权限系统不完善;
- 3) 隐私保护难;
- 4) 合规要求高;
- 5) 行业定制化需求多;
- 6) 普及度低;
- 7) 上手门槛高;
- 8) 生态不完善。

在区块链商业化落地的过程中，想要真正构建基于区块链的价值互联网体系，赋能至各行各业，就需要从技术框架、产品体系、生态建设、应用实践四个方面同时发力，解决目前所遇到的系列瓶颈问题：

- 1) 技术框架：应具备性能稳定可预期、通用性好、多业务适配、合理的分层解耦等要素；
- 2) 产品体系：应具备商业化一站式能力，可支持行业用户的区块链化，提供必要的功能闭环和多场景适配能力；
- 3) 生态建设：应在区块链安全、区块链工具、区块链业务适配等领域形成合作伙伴矩阵，加速商业化落地；
- 4) 应用实践：应具备价值可衡量、通用性、模板化、行业灵活适配等核心能力。

3.1.3 百度区块链商业化布局



图 7 百度区块链的商业化体系布全景图

百度云融合百度区块链实验室的最先进技术，在区块链商业化进行全面地探索和实践。百度的区块链服务（BaaS）结合云计算的资源、部署、交付和安全等系统能力，将区块链平台进行云端系统化和产品化，并有序地输出至金融、物联网、游戏等行业，赋能合作伙伴，构建行业区块链的战略联盟和标准。

（1） 百度区块链商业化的定位和价值主张

百度区块链商业化定位于云端一站式的区块链赋能中心，为企业用户提供开箱即用的区块链技术和产品能力，提供可信存证、数字版权、清算结算、供应链金融、数字资产、区块链游戏等多场景的模板化服务，赋能区块链在金融、物联网、游戏等多行业的落地。

百度区块链商业化的价值主张是技术赋能、生态联盟和价值分享，在区块链普及化、服务化、生态化方面与合作伙伴一同贡献力量。

（2） 百度区块链商业化的优势和创新

百度区块链商业化的优势和创新体现在技术、产品和实践等多个方面，技术上提供多场景覆盖多标准兼容的统一框架，拥有立体链网架构、网络多租户、单链高并发、单系统多框架、跨链等场景需求的支撑能力，产品上具备超级节点、私有部署、应用托管等多形态，同时支持云端输出百度各业务线的区块链先进实践，如百度百科、图腾、度宇宙等。

3.1.4 百度云区块链的产品和技术框架

百度云作为区块链商业化的实施主体，拥有全面完善的产品和技术体系。

（1） 百度云区块链产品系列

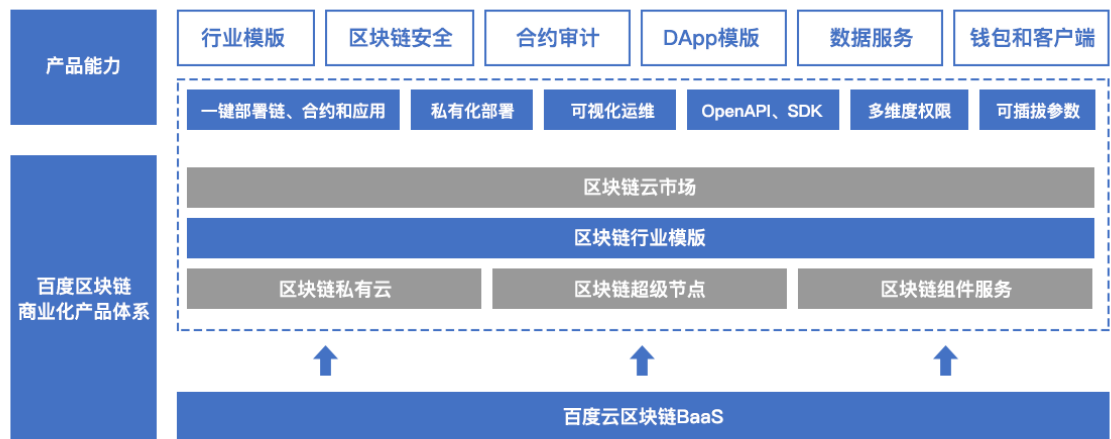


图 8 百度云区块链产品系列示意图

1) 百度云 BaaS

百度云 BaaS，是云端一站式的区块链即服务产品，用户通过购买资源、搭建区块链网络、编写智能合约、构建去中心化应用 DApp，即可搭建出属于自己的区块链系统和应用。

- ① 提供区块链核心功能：账本、合约、鉴权和共识，支持可升级的区块链参数，提供区块链系统的全部核心要素；
- ② 提供区块链云能力：一键部署、云端托管、安全监控、账户权限等，提供基于云的一站式区块链系统交付能力；
- ③ 提供实践模板：合约模板、DApp 模板，将百度区块链版权、游戏、社区、金融等成熟区块链解决方案开放给企业合作伙伴。

2) 区块链超级节点

百度云超级节点，是区块链能力集合，支持软硬一体或者纯软件的交付形式，提供开箱即用的区块链系统。

- ① 提供基础的区块链能力集合：最小化完整的区块链网络能力，包括节点、账本、共识、合约和应用等；
- ② 提供与公有链、BaaS 等区块链平台进行可信交互的能力；
- ③ 支持差异化场景选择：包括自定义记账节点、监督节点、查询节点、跨链通信等。

3) 区块链私有云

区块链私有云，提供分层级的私有区块链云框架，底层云平台支持容器化的部署安装和原生云能力，上层区块链网络支持用户根据场景选择所需的区块链能力，是功能完善的私有化系统平台。

4) 区块链组件服务

百度云提供一系列的区块链组件服务，如节点托管服务、密钥保险箱、全节点服务、轻量级节点服务、侧链和跨链服务、合约审计服务等，助力云端区块链生态的完善。

5) 区块链云市场

区块链云市场，支持合作伙伴一键式发布、售卖、运维各种区块链服务，同时提供云市场服务与百度云 BaaS、超级节点和私有云的数据同步、服务连接、以及激励生态共享等能力。

6) 区块链行业模板

行业模板将提供系列区块链场景实践，如区块链数据共享平台、催收任务分包平台、物流可信信息存证平台、合规激励系统平台、资产证券化平台、供应链金融平台等，百度云支持行业模板的云端输出，赋能合作伙伴，加速区块链商业化落地。

(2) 百度云区块链技术框架

百度云区块链技术框架是为了解决百度区块链商业化落地，而设计研发的一套完整的区块链商业化技术栈，提供了如下技术能力：

- ① 使用一套可复制可插拔的统一技术栈来满足不同区块链业务场景需求；
- ② 支持私有化的区块链落地环境；
- ③ 支持多样的区块链框架、区块链形态；
- ④ 支持多组织链上账户体系和身份互信机制。

1) 百度云区块链总体技术框架

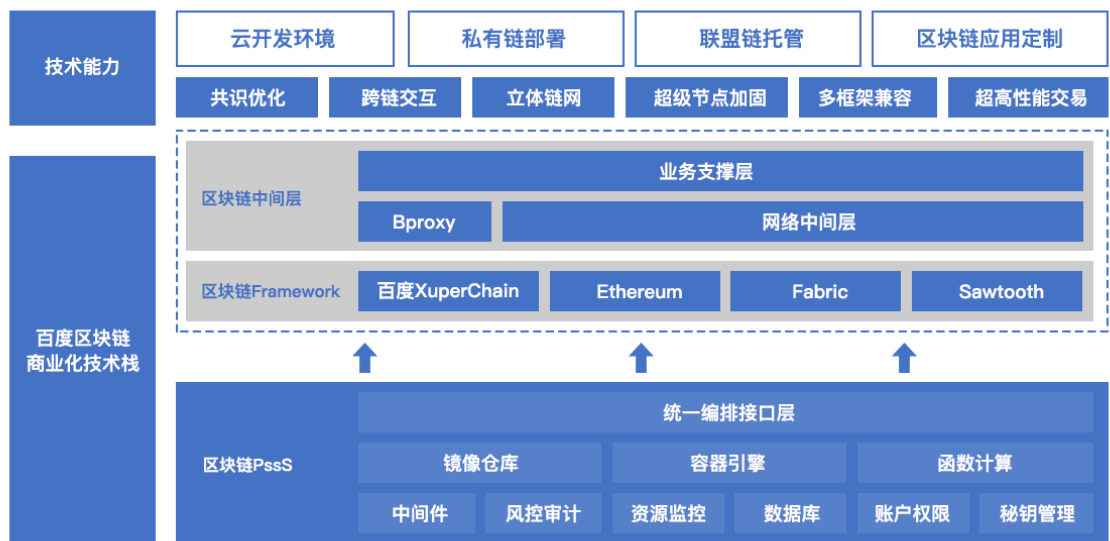


图 9 百度云区块链商业化技术框架

整体技术框架分为两大部分：百度区块链商业化技术栈和商业化技术能力。技术栈核心主要包括三大部分：区块链 PaaS、区块链 Framework、区块链中间层。百度云区块链平台是由这三层技术栈合力驱动的，形成一个完备的商业化技术方案。

2) 区块链 PaaS

区块链 PaaS 是为了解决商业化环境的差异性问题。PaaS 层能够对上层的区块链 Framework 屏蔽资源环境因素，引入了基于 Kubernetes 和 docker 的容器集群引擎、镜像仓库和函数计算等能力，实现了计算和存储资源的统一化抽象和高效利用，还提供了镜像级的版本管理和函数式的合约编程框架。

区块链 PaaS 在顶层封装了统一的编排 API 层。编排 API 整体面向资源，包括函数计算任务资源、镜像资源、实例容器资源和其它基础资源。统一资源调度动作描述和描述结构体。可以简化上层 Framework 调用不同服务的复杂性。

3) 区块链 Framework

区块链 Framework 层主要解决三个问题：

① 多种区块链网络的兼容部署

在节点部署、合约部署、DApp 部署全流程中支持 XuperChain 的一键部署，同时也支持以太坊、Fabric 等其他开源框架。

② 多种区块链网络的托管和监控方案

区块链 PaaS 层提供了资源 failover 策略保证网络节点故障可自动恢复还提供了不同区块链框架的兼容性监控方案，指标包括链上区块数、出块速度、单位块验证速度、每秒交易数 TPS、每区块交易数、子链数、跨链交互次数、机构数等。

③ 多种区块链网络的交互逻辑抽象

部署区块链网络的流程可以归纳为配参+部署的交互逻辑，其中配参包括的参数项有：框架类型、联盟参与方信息、网络规模、账号、合约和 DApp 等信息。

平台将使用 framework 预设逻辑调用区块链 PaaS 接口进行一键式部署。

4) 区块链数据 BProxy

区块链 BProxy 为一个代理模块，解决了多种区块链方案私有化场景的适配问题，实现多方的身份互信管理，同时也在跨网环境中解决了数据上链的问题。

5) 区块链网络中间层

不同的区块链框架偏向不同的交易类型，区块链网络中间层完成了跨链数据的结合读写，通过与不同类型的区块链网络交互完成多类型数据的事务性同步，直接与 DApp 进行数据交互。

6) 区块链业务支撑层

区块链业务支撑层主要为了将不同业务应用与底层区块链方案进行实际解耦，支持数据和签名的差异化存储上链，提供场景化的身份定义，同时平台在业务支撑层增加了通用的合约基础库和合约模板。

3.2 百度区块链行业落地案例

百度云区块链场景布局全面，从轻量级的可信存证到风险系数较高的金融业务，具备全面实施能力和实践经验。

(1) 可信存证和查询

区块链提供了链上数据不可篡改，共享可查的链上记录等能力，百度云在数字版权、信息共享平台等区块链应用领域拥有场景实践。

(2) 可信的积分激励型应用

百度云结合度宇宙、图腾积分等 DApp 实践，拥有合规框架下的通证激励解决方案。

(3) 数字资产创造和管理

百度拥有云端构建数字资产平台的全套方案，同时提供相应的合约和 DApp 模板，支持一键式构建用户专属数字资产区块链网络。

(4) 多方协作，信任达成，附加金融

区块链提供了多方信任和数据共享机制，百度在资产证券化 ABS、供应链金融、信用卡催收等方向拥有先进的落地实践。

(5) 清算、结算和支付

我们在区块链平台技术的性能和安全性上持续发力，结合百度自研的超级链技术，在跨境支付和金融清算结算上拥有前瞻布局，平台可支持百万以上 TPS，支付延迟可到达秒级。



图 10 区块链落地场景

百度云区块链系统在金融、物联网、游戏等多行业拥有最佳实践，下面将给出两个创新的百度云区块链场景案例。

3.2.1 金融区块链场景案例

以金融行业为例，在信用卡催收、零售信贷催收等场景中，存在信息透明度不高、平台地域分散、无有效激励体系、招标合同流程繁琐、结算周期长等问题。通过私有化部署了百度云区块链平台，金融机构将催收分包任务上链，实现了全流程的信息共享、真实和透明，借助链上合规通证体系，为第三方合作伙伴构建了一套以贡献度为准的激励体系，同时规避了以往招投标、结款等繁琐流程，大大提升了催收效率和平台信任度。

另外，该套系统也是 AI+区块链的很好实践，通过对接百度提供金融大脑技术，将用户画像和机构数据进行分析和建模，寻找到了最合理的定价和激励标准，大大提升了效益产出。

(1) 催收任务可信分包平台

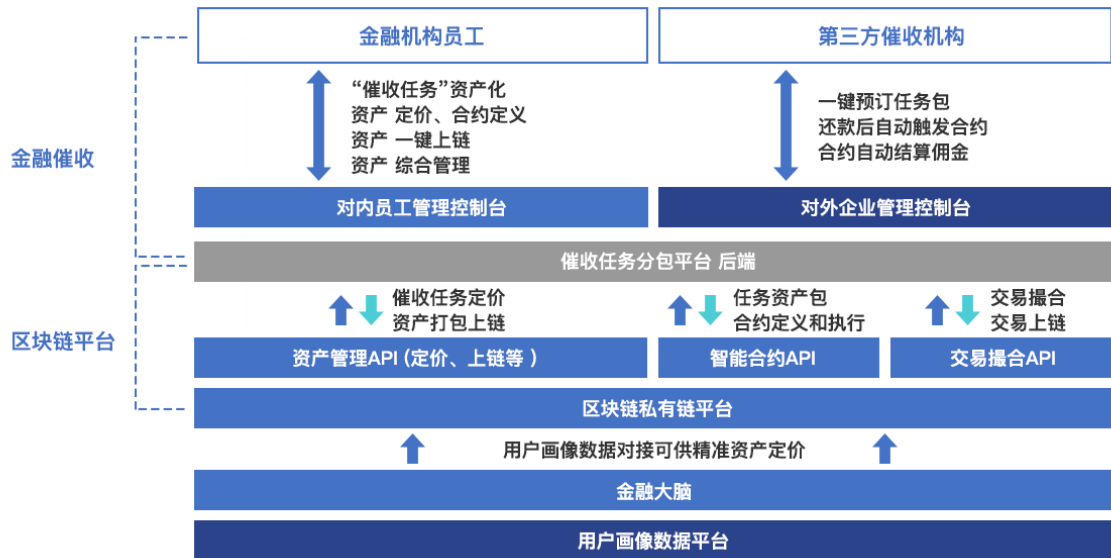


图 11 催收任务可信分包平台

3.2.2 物联网区块链场景案例

(1) 能源物联网场景

随着能源企业在精细化、商业化方向上的发展，对可信和效率的需求显著提升，借助区块链本身的数据不可篡改、智能合约结算效率高等特性将帮助政府更好的进行监管，指导行业健康发展。

百度云区块链从园区出发，将智能电表、微网、发电以及配电设备等结合起来，形成打通发配售的园区能源系统，将园区政府、企业、应用、服务提供商以及环评机构等的信任体系和交易系统搭建在区块链之上，形成园区能源账本，实现日前和日内现货交易、需求侧响应等。构建了区域性的大型新能源网联生态。

1) 解决痛点：

- ① 能源资产数字化可溯源，能源的设备生成、流通环节全透明；
- ② 能源长协合同和现货交易不可篡改，以及公开透明；
- ③ 符合政府监管要求以及环保价值。

3.3 百度云区块链的发展规划

百度云区块链会经历四个阶段，完善百度区块链云端赋能中心：

第一阶段：构建区块链统一云平台，云平台具备多框架、PaaS、区块链定制优化等能力。

第二阶段：商业化的区块链应用开发和托管，提供存证溯源类、积分激励类、数字资产等多类智能合约和 DApp 模板，构建兼容性好的私有链、联盟链统一技术框架。

第三阶段：完善框架与交付形态，支持更多区块链框架、可插拔共识机制、立体链网架构（单链分片、多链可信交互、侧链）增强型合约虚拟机等能力。

第四阶段：区块链与云的深度结合

当区块链云平台的商业场景规模化过程中，如何加强区块链云平台基于云原生的先天优势，是一个需要持续发力探索的领域，如区块链与边缘计算、云安全、人工智能等解决方案有很好的先天互补特性。

- （1） 区块链+边缘计算：边缘设备处理数据和分析的方式，是可信溯源等区块链场景的设备端技术基础，可提升上链过程中的安全、可信和自动化程度，同时大量具有计算能力的设备加入区块链，会有效提升网络规模与算力；
- （2） 区块链+安全：云端安全技术可以助力公开节点抗攻击的能力，云端加密框架和验证模型能够对接区块链网络中的数据入口，通过强制数据加密和签名验证的策略，增强上链可信度；
- （3） 区块链+人工智能：人工智能提高了生产力，区块链改善了生产关系，人工智能可对链上数据进行分析、训练、模型化和再利用，同时链上数据则通过分散控制和数据多方共享，充分保证了人工智能数据来源的可信。

区块链与云平台的深度结合将充分挖掘云服务的计算潜力，同时将云原生的优势赋能区块链网络，但仍有很多挑战，将是一个持续的技术课题。

第四章 百度区块链行业应用

基于超级链技术，百度已经开始积极探索区块链在各行各业的应用。本章节描述百度在 2018 年上半年开展的部分尝试。

4.1 内容版权

4.1.1 内容版权领域的发展趋势

内容版权行业主要指网络中有价值内容的版权注册以及依托版权保护，进行内容创造、发行、分发及 IP 衍生金融交易等相关业务领域。其中，有价值内容包括文字、图片、视频、音频、数据（云盘、无人车等行业高价值数据）等多种类型的表现形式。

根据国家版权局网络版权产业研究基地 2018 年 4 月 23 日发布的《中国网络版权产业发展报告(2018)》显示，2017 年我国网络版权产业市场规模达 6365 亿，较 2016 年增长 27.2%。

4.1.2 内容版权领域的痛点

内容版权行业高速发展的同时，也暴露出了版权内容确权成本高、盗版猖獗和交易效率低等行业问题。

（1） 确权成本高

内容版权生产者耗费大量精力和财力创作出的内容作品，投放到互联网平台可迅速获得广泛的网络传播，但却很难确定版权归属。如果创作者通过政府版权机构申请版权归属，又面临着周期长、成本高、手续繁琐的问题。每日互联网平台诞生数以百万计原创作品的确权问题，一直困扰着创作者和版权机构。

（2） 盗版猖獗

当前网络中内容作品被盗用的现象屡见不鲜，主要原因在于侵权发现难和维权难。

侵权发现难：互联网上的内容作品因其本身易修改、易流通的特性，极易被二次加工和二次传播，当缺乏公开健全的侵权检测机制时，侵权行为很难被发现。

维权难：发现了侵权行为后，盗版线索是否能够维权，如何找到维权机构，如何维权，都需要内容创作者花费大量精力去研究，可谓困难重重。

（3） 交易效率低

内容平台是连接创作者与用户的桥梁。面向创作者的版权平台因为缺乏流量，不能使版权内容得到充分的分发、曝光和交易。拥有流量的分发平台，以平台自身发展为导向，对原创内容存在喜恶偏见，向平台主流用户的小众审美和成熟内容创作者倾斜，限制新兴优质作品价值发现，对新晋创作者不友好。此外，中心化的平台还存在着信息不透明，平台盘剥创作者，收益分配不公平的问题。

4.1.3 内容版权的区块链解决方案

针对版权行业“确权成本高、盗版猖獗、交易效率低”的痛点，百度结合区块链技术、搜索技术和流量的优势，构建起全新的内容版权生态平台（图腾）。

（1）图腾的价值主张

让人人的数字资产得到版权保护、产生版权价值。

图腾以先进的区块链技术作为底层支撑，秉承绝对开放公正的原则，让互联网原创内容上传、使用及交易体系化、透明化，享有全流程的版权保护权益，借助百度搜索的力量，使原创内容触达各行各业的亿万用户，充分获得品牌曝光和流量，让每位参与者均能受益，提升内容版权行业效率，实现行业价值的最大化。

（2）图腾的产品优势

1) 平台优势

百度作为国内一流的搜索引擎，具有全面的用户基础和巨大的流量，并且非常重视原创内容生态。依托百度平台的优势，能够使优质原创作品高效触达各行各业的用户，为版权作品提供更多的落地场景和流量导入机会。

2) 技术优势

百度先进的超级链技术，为内容版权行业提供强有力的体系化支持，助力版权行业全流程更加公信、公开、透明。

百度先进的人工智能技术，基于语义理解、图像分析、视频理解、内容聚合等多项技术能够快速构建智能推荐和检索系统，助力版权内容触达亿万用户。

3) 品牌优势

合作者成为百度区块链战略合作伙伴，可提升自身品牌的权威性和影响力，在内容版权行业趋于激烈的竞争中具有更多优势。

（3）图腾的产品功能

1) 全流程的版权保护

将作品版权信息永久写入区块链，基于区块链的公信力及不可篡改性，结合百度领先的人工智能盗版检测技术优势，让作品的传播可溯源、可转载、可监控，改变传统内容版权保护模式。

2) 多渠道的内容分发

基于语义理解、图像分析、视频理解等多项人工智能技术，构建版权内容的搜索和推荐系统，依托百度系产品流量支持，精准匹配版权内容与用户需求，实现版权内容供需双方高效连接。

3) 技术赋能的原创生态

建立基于区块链技术的版权登记系统、盗版检测系统和版权内容检索系统，发挥百度技术生产力，赋能原创作品版权登记、监控与维权。

4) 助力提升行业效率

基于区块链上链信息的公开透明性，解决行业信息不对称、流程效率低等切实痛点，打破封闭旧模式，实现版权内容行业的高效率及专业化。

(4) 图腾的实现方法

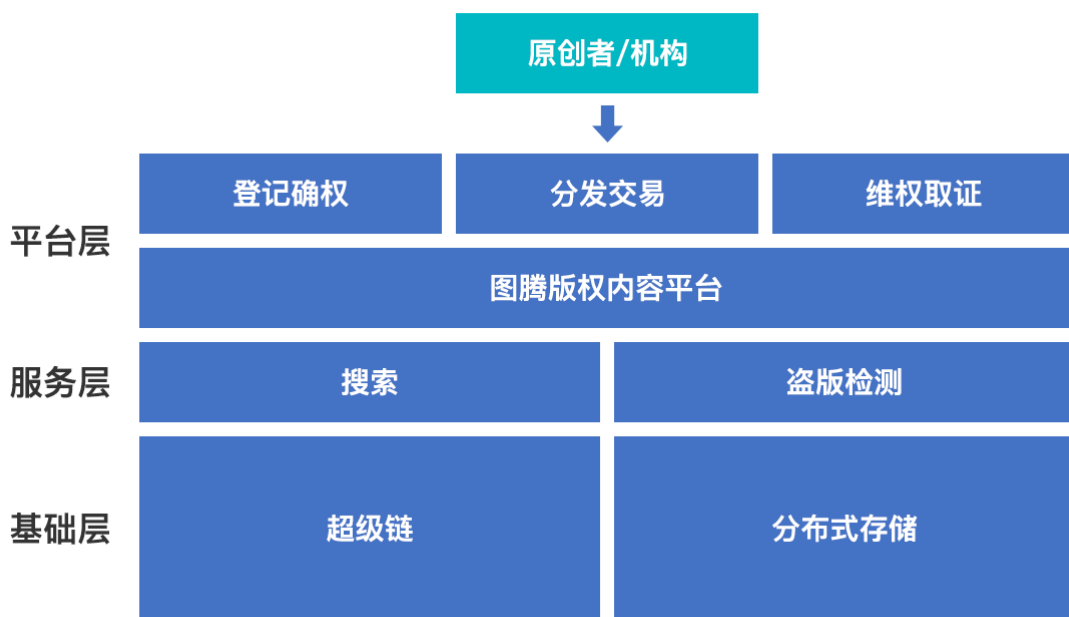


图 12 图腾的技术架构图

- 1) 基础层：基于百度超级链技术构建版权链，版权链用于记录版权行业登记确权、维权线索、交易等需要公信力或透明性的信息，版权链由百度、内容机构、确权机构、维权机构等节点共同维护和账本同步，具有强大的公信力。庞大的版

权内容信息则是存储于百度分布式存储系统中。版权链和分布式存储系统中的内容可相互关联访问；

- 2) 服务层：构建搜索、盗版检测等基础服务。搜索：针对上链的版权内容，根据资源类型，构建文本、图片、视频等多种类型的搜索系统，为原创内容购买者提供一个需求匹配的便捷入口。盗版检测：基于百度强大的技术背景和丰富的网络资源，利用成熟的分布式爬虫系统，对全网资源进行采集。基于智能 AI 技术，构建文字、图片、视频的重复检测系统，利用强大的算法和过硬的技术，即便内容发生了部分修改也能被追踪和发现；
- 3) 平台层：为内容生产者提供登记确权、分发交易、维权保护等核心产品功能。

(5) 图腾的积分体系

图腾积分是图腾平台为激励用户原创内容上传、信息上传等行为所发放的具有一定可兑换价值资源和权益的积分。图腾积分初始生成40亿，按照一定的规则由图腾区块链系统公平、公正、自由的进行发放，发行对象是所有图腾个人或者机构用户，每年新增发行一定比例的图腾积分，作为版权链节点记账的奖励。图腾积分的宗旨是用经济激励赋能内容版权生态，同时在百度生态内部可进行通证的流转及兑换相应权益。

4.1.4 内容版权未来的发展规划

目前，图腾平台已率先完成了图片版权区块链完整解决方案的实现，对图片版权行业提供了版权保护和交易的全流程支持。

未来，图腾计划将平台能力从支持图片扩展到支持文字、视频等更多类型的版权内容表现形式。并与百度云盘合作，让人人的数字资产得到版权保护，产生版权价值。

4.2 信息溯源

4.2.1 互联网信息领域的痛点

随着互联网的快速发展，进入“数字时代”以后，全球信息量每两年翻一番，信息传播呈现出碎片化、原子化的特征。信息爆炸式的增长，使信息的获取过程更便捷，解决了信息不对称的问题，但相应的也产生了一系列问题：

- (1) 信息来源的多元化导致信息本身的可靠性下降

信息来源渠道越来越丰富，社交媒体、自媒体等新兴媒体渠道不断涌现，可以说“人人都是信息源”。其中有一部分人，为了博眼球刻意发布不实信息，导致互联网上的信息良莠不齐，信息本身的可靠性大大下降。

（2） 信息传播成本下降导致内容的权威性、正确性无从考证

移动互联网等新兴技术的赋能，使信息二次传播的成本大大降低，通过复制粘贴、转发等手段可以轻松的将信息多次传播，加剧了信息源头追溯的难度，导致内容的权威性、正确性无从考证。

如何让内容更可信，已成为内容产业迫切需要解决的问题。而解决这一问题的方式之一，就是信息溯源。

百度百科是全球最大的中文网络百科全书。它强调用户的参与和奉献精神，充分调动互联网用户的力量，进行知识的交流和分享，旨在创建一个涵盖各领域知识的中文信息收集平台。与此同时，百度百科倡导编辑者们秉持“真实、客观、负责”的原则，为亿万网友提供正确、全面、更新及时的知识内容。百度百科将通过信息溯源的方式，实现词条内容的去伪存真。

4.2.2 百度百科在信息溯源的区块链解决方案

（1） 百度百科内容正确性的现存风险

百度百科是由网民共同参与编辑的网络百科全书平台。截止 2018 年 6 月，累计 654 万名用户参与词条编辑，共形成 1542 万个词条，1.4 亿个版本。百度百科词条的内容均是以多人协作、版本迭代的方式逐步编写而成。用户的每次操作，如创建新词条或修改词条内容，均会形成一个新的版本。通过版本的不断迭代，一个词条才逐步趋向完善。

为了保证词条内容的正确性，百度百科把单个词条所有审核通过的版本按照时间顺序排列，形成该词条完整的编辑记录，实现编辑者、编辑时间、编辑内容可追溯。词条编辑记录供全体网民公开查阅，当发现词条内容存在争议、错误和风险时，就可以“顺藤摸瓜”追溯到内容的源头版本及其编辑者。

可见，词条编辑过程可追溯是百科词条内容正确性的基础保障设施。然而，当前词条编辑记录的公正透明性还无法得到各方的共同认同。因为，目前词条的编辑记录均存储在百度的服务器上，这是一种中心化的存储方式，很多人因为自身的利益恶意攻击百度随意修改词条。在信任缺乏的情况下，这份数据不能作为信息溯源的有效依据。

（2） 百度百科与区块链技术的结合点

区块链技术是把数据在多个节点存储副本，由于其通过共识机制实现节点信任，数据变更需要经过其他节点确认，因此能够有效地应对数据篡改、数据伪造的风险。

百度百科启动词条编辑记录区块链化的项目，运用区块链技术“不可篡改”的特性，形成各方共同认可的、可信的词条编辑记录。再借助词条编辑记录的溯源能力，监督词条的编辑行为，追踪风险内容，维护词条的正确性。

区块链能力赋能下的百度百科相比同类百科类产品，最大的优势在于：修改历史能够被可信地溯源——通过历史版本记录及区块链信息，可以准确可信地确认词条中每一个事实、每一句描述的编辑者。

(3) 百度百科与区块链结合的技术实现方法

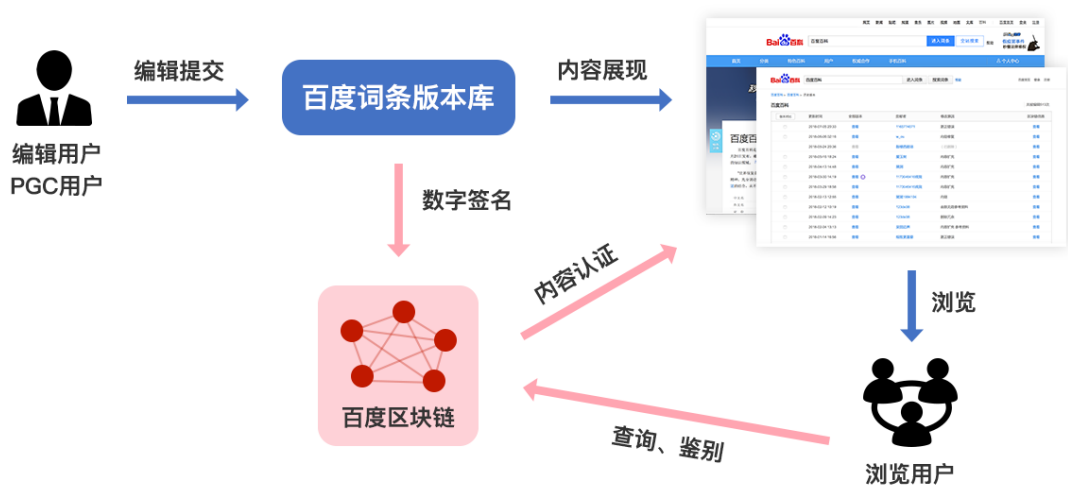


图 13 百科区块链业务逻辑

百度百科区块链业务逻辑如图 13 所示，蓝色部分表示百科内容编辑的业务流程，红色部分表示区块链相关业务流程。

整个业务逻辑在现有百科内容编辑的流程下，实现了区块链功能：在用户提交词条版本后，将版本内容的签名信息写入百度区块链，以提供对用户版本内容的认证能力。在历史版本页面新增“区块链信息”入口，用户可以主动发起对区块链信息的查询和鉴别。

(4) 百度百科词条编辑记录功能介绍

百度百科 > 百度(百度公司) > 历史版本

百度 共被编辑648次

版本对比	更新时间	全部版本	贡献者	修改原因	区块链信息
<input type="checkbox"/>	2018-05-18 18:23	查看	龔从东来	更正错误 排版	查看
<input type="checkbox"/>	2018-05-18 18:18	查看	龔从东来	排版 参考资料	查看
<input type="checkbox"/>	2018-05-18 18:18	查看	龔从东来	排版 参考资料	查看
<input type="checkbox"/>	2018-05-18 18:12	查看	龔从东来	更正错误	查看
<input type="checkbox"/>	2018-02-28 10:54	查看	yz_candydu	更正错误	查看
<input type="checkbox"/>	2018-02-26 20:56	查看	yz_candydu	内容扩充	查看
<input type="checkbox"/>	2018-02-22 15:33	查看	yz_candydu	排版 内容扩充	查看

图 14 编辑记录界面新增区块链信息

每当用户提交的新版本被审核通过时，词条会被更新，同时会自动生成一条编辑记录，包括：更新时间、更新内容、贡献者、修改原因等。新增功能如图 14 所示，该条编辑记录的特征信息同时被存储到区块链上。用户点击区块链信息列的“查看”链接，就可以查阅存储在区块链上的信息。

百度 共被编辑648次

版本对比	更新时间	区块链信息	区块链信息
<input type="checkbox"/>	2018-05-18 18:23	查看	查看
<input type="checkbox"/>	2018-05-18 18:18	查看	查看
<input type="checkbox"/>	2018-05-18 18:18	查看	查看
<input type="checkbox"/>	2018-05-18 18:12	查看	查看
<input type="checkbox"/>	2018-02-28 10:54	查看	查看
<input type="checkbox"/>	2018-02-26 20:56	查看	查看
<input type="checkbox"/>	2018-02-22 15:33	查看	查看

区块链信息

版本哈希值: 342e5048dd08af609c02ff549d04bf91
词条版本号: 128326625
更正时间: 2018-05-18 18:23
贡献者: 龔从东来

所在区块链信息

区块高度: 234180
创建时间: 2018-05-23 22:48
哈希值: 5dbaf960e8cfb09651204d97c529cd575959c0305e22fe5bddf0d55f64ca9477

图 15 区块链信息查询界面

存储到区块链上的编辑记录，分布式存储在多个节点。多个节点的数据通过区块链的共识机制相互印证，避免了百度单方面篡改区块链上的版本特征信息的风险，并且可以通过版本内容重新计算版本特征信息，与区块链上的数据进行比对，保证编辑记录数据的公正透明性。

4.2.3 百度百科未来的发展规划

为保证词条内容正确性，百度百科不仅要实现词条编辑记录可追溯，还鼓励用户在编辑词条时只参考可靠的信息源，并以“参考资料”的形式记录该信息源，从而实现内容来源可追溯。

运用区块链不可篡改的特性，百度百科首先将用户编辑更新的内容及引用的参考资料上链，实现第一层内容来源存证。再通过 AI 技术分析、原创登记、与其他内容版权链开展合作等多种方式，实现更进一步的来源追溯和存证。

这样，用户在阅读百科词条时，可以清晰地看到词条内容的原始来源地址，便于其进一步拓展阅读。此外，一旦发现某内容源不可靠，百度百科可通过区块链快速定位风险内容并予以处理，有效维护词条内容的正确性。

以百度百科为代表的互联网内容平台，在信息溯源领域应用区块链技术，可以实现内容有源可查、溯源过程可信。从而让内容更真实、更透明。在未来，百科还计划与各个行业区块链打通，通过 AI 技术将区块链中的可信数据直接转换为相关词条，进一步保障百科信息的真实性和权威性。

4.3 文化娱乐

4.3.1 文娱产业现状

文化娱乐是精神文明建设的重要组成部分。随着互联网的兴起，大量文化娱乐以数字化的方式存在，比如各种网游、页游和端游，以及网络社区和论坛。用户在其中投入了大量的时间和心血，创造了一个个平行的数字世界。这些传统文娱应用经常会遇到各种挑战。

（1）安全性问题

在传统文娱应用中，隐私泄露、数字资产被盗等事件频发，用户信息安全得不到保障。而一旦应用不再运营，用户在该款应用中的虚拟资产也将丧失。

（2）透明性问题

游戏中的稀有道具的抽取概率、直播平台的真实观看人数等等，在现有的产品运营体系下并不会完全公开，影响了产品的可玩性和公平性。

（3）公平性问题

在传统游戏应用开发中，开发者往往处在上帝的视角，可以随意通过更改规则侵犯玩家的利益来达到自己利益最大化。而不是在一个合理的规则下，通过改善游戏体验来使自己利益最大化。从而让这个行业鱼龙混杂。

区块链一个非常显著的特点，就是擅长对数字资产进行创建和管理。因此，现在诞生了不少数字社区、游戏与区块链结合的创新应用。但这些区块链文娱应用也面临新的困境：

(1) 日活量极低

以游戏为例，目前市场上基于 ETH 的区块链游戏，只有少数表现稍好的游戏 DAU 达到 100 左右。整体区块链游戏市场处于低迷状态，并没有吸引到真正的用户群体。

(2) 内容单一，质量低下

区块链文娱应用市场存在简单化、同质化问题，加之游戏厂商对区块链的认识不足和赚取快钱的逐利心理，很难产生具有吸引力的优质游戏。

(3) 资产炒作的嫌疑

因为区块链让游戏很多道具成为数字资产，很多投机分子直接炒作游戏的数字资产，而不是真正为了做好一款游戏。

4.3.2 度宇宙的产品定位

度宇宙作为百度超级链的首款原生应用，旨在成为全球最大，真正具备用户价值，以区块链为基础的文娱应用生态平台，构建一个集“区块链+大数据+娱乐+社交+消费”于一体的数字世界。度宇宙将通过构建丰富的应用场景，让用户在体验中认知和体会到区块链的价值和优势，从而获得更高质量的娱乐体验。

4.3.3 度宇宙解决方案

(1) 结合区块链的优势

- 1) 度宇宙将资产信息上链，基于区块链的分布式记账特点，有效规避对单一节点的攻击导致的数据丢失问题。同时，区块链上的数据永久存在且不可篡改，用户的资产也就永久存在；
- 2) 链上信息公开透明，度宇宙项目方无法进行数据造假、滥发商品和道具，使用户具有更平等的权利，进而规避传统模式中的矛盾和纠纷。

(2) 依托百度的优质资源

- 1) 度宇宙依托百度平台的庞大用户基础，快速吸引用户入驻，并为用户分发精品内容。通过盘活度宇宙内的生态，未来可以为海量应用提供精准的流量导入。

2) 度宇宙已和多家机构、团队建立深度合作关系，依托百度站内丰富资源和庞大的生态体系，助力合作伙伴开发优质应用，并一起分享用户红利，共同促进生态繁荣。

1) 系统架构设计



图 16 度宇宙的系统架构

① 存储层

度宇宙架构在区块链和分布式存储系统上，关键逻辑使用智能合约实现，核心数据则通过智能合约写入区块链，并将内容数据存储到分布式系统中。

② 服务层

构建竞猜、PK、知识等系统服务，为星球主提供基础服务，构建元素市场。

③ 平台层

社区开发者可以通过度宇宙对外的开放平台接入，在度宇宙上贡献知识，进行星球经营，最终共建用户兴趣社区。

2) 成员管理

度宇宙采用 DPOS 共识机制，由宇宙居民投票选举出若干超级节点，超级节点持有者将共同组建度宇宙理事会。理事会是度宇宙中的最高决策机构，其决策事项包括但不限于：决定社区发展方向、调整元素分发比例、核心技术的变更及升级、紧急决策和危机管理议程、星球运营权的授权等。通过全民参与，让用户而不是中心化节点来决定度宇宙的整体发展。

3) 产品规则

① 基本概念

元素：它是度宇宙生态中的权益证明，可通过引力进行凝聚，或者通过指定的系统行为获取。

引力：它是度宇宙中目前探索到的一种力量形式，可凝聚元素。引力越大，就能获得越多的元素。它本质是用户在社区中的决策权益。

星球：来到度宇宙的居民会有创世力量为其凝聚一颗独一无二星球，是居民的个人资产载体。用户可以通过星球来搭建自己的专属社区。

② 居民玩法

a) 星球升级

星球在第一宇宙纪元中分为 9 个等级，用户可通过完成指定的系统行为进行星球升级。每次升级，星球的外貌也会随之变化。当星球提升到一定等级时，会开启不同功能。星球最终成型的状态总共有 12 种形态，最终形态是根据居民的偏好不断衍变出来。

b) 星球装扮

在宇宙道具商城中，用户可以购买一些道具，如卫星、光环等装扮自己的星球。

c) 星际探索

宇宙居民可以从自己的星球出发，穿越虫洞，开始星际旅行，在旅行过程中可以任意着落探索到的星球。

d) 价值生产

宇宙居民可以在内容开放的星球成为生产者。生产者的主要任务为星球应用提供价值内容，最后获得元素奖励作为回报。依托于百度强大的商业变现能力和内循环系统，度宇宙能产生真实的商业价值，让元素具备实际意义。

(3) 星球运营

a) 竞选星球经营者

度宇宙理事会将挑选优质的合作方，通过社区投票，由宇宙居民选择认可的经营者获取星球运营权。

b) 星球排行榜

为保证星球运营质量，理事会根据应用类型和运营情况建立星球排行榜。排名靠前的星球，其经营者将获得元素奖励。

4.3.4 度宇宙未来的发展规划

度宇宙将在 2018 年下半年内为用户创造更多爆款模式，丰富应用场景，增加产品流量；并在 2019 年完成平台自身的基础建设，开放平台接口，构建分布式协作的内容创作机制，与各路精英一起构筑宇宙生态的护城河。根据娱乐产业的发展需求和特点，度宇宙致力于为用户打造一个真正的数字社区，成为数字原住民概念的布道者和实践者。

4.4 信息安全

随着全球信息化快速发展，信息化已渗透到社会生活的各个领域，信息安全问题也日益显著。习近平总书记在今年 4 月全国网信工作会议上指出：要决心、恒心、重心，加速推动信息领域核心技术突破。反恶意软件是信息安全的一项基础技术。反恶意软件与恶意软件的战斗，经历了个人计算机时代，互联网时代，移动互联网时代，到现在的人工智能时代和物联网时代，战斗不但没有结束，反而愈演愈烈。

4.4.1 反恶意软件行业的痛点

仅在 2017 年，发现的新增恶意软件数量在 PC 端超过 1 亿个，移动端超过 1 千万个，感染终端总数达亿次。其中“WannaCry”勒索病毒袭击了全球至少 150 个国家的 30 余万用户，造成损失高达到 80 亿美元，包括政府部门、教育、医院、能源、通信、制造业等多个行业领域受到攻击感染。安卓病毒“Judy”，全球范围被植入超过 3600 万台安卓终端，以入侵手机窃取信息的方式来点击广告并获取利益，超过 40 个 Google Play 商店应用被捆绑了该恶意软件。当下，反恶意软件行业痛点包括但不限于如下三个层面：

（1）反恶意软件技术亟待升级

反恶意软件技术（或称为反病毒技术），从诞生起就有天生的缺陷：即必须收集到恶意软件的相关信息，才能产生具有检测这款恶意软件（特征或签名）的具体方法。从恶意软件被制作出来、传播出去、感染宿主、发作运行，到被感知、被收集、被分析、能检测、检测特征并分发到用户，这已经经历了一个十分漫长的过程。也就是说对恶意软件的检测是严重滞后的。近年来流行的针对国家基础设施实施攻击的 APT（高级持续性威胁）类高级恶意软件，为了不让自己被反恶意软件技术感知到，感染宿主之后会长期潜伏在宿主机上不作发作，潜伏期可长达数年之久。即使对软件的行为进行监控，也很难及时发现此类恶意软件。

反恶意软件和恶意软件的战斗已经持续了超过三十年，但是在技术对抗层面，恶意软件总是能够抢占先机。正所谓是道高一尺，魔高一丈。恶意软件在逃避检测方面无所不用其极，呈现出了自动化免杀、加固、动态加载等多种技术特点。而各种恶意软件的制作工具不断出现，进一步降低了恶意软件的制作门槛：生成速度快，变种繁多。传统反恶意软件引擎使用的以特征签名，云端情报检测的方式，疲于应对各种新技术恶意软件。因此，出现了响应不及时、0Day 病毒处理慢、止损困难、对抗不足等现状。反恶意软件技术亟待升级。

(2) 缺少可信高价值社区

当前软件公司、安全厂商、分发渠道、终端厂商、个人用户、政府用户、企业用户等之间还未建立成熟的信任机制，使得恶意软件有机可乘，威胁用户安全。对于软件信息、情报信息等大数据未形成有激励的交换机制，使得数据既重复存储，又不对称。当黑客越来越产业化、商业化运作时，反恶意软件成员也应团结力量，建立可信任、富有价值的安全社区，以形成有力的对抗组织。

(3) 普通用户参与度不足

用户是恶意软件攻击主要的受害方，但目前用户对于反恶意软件参与度不足。恶意软件鉴定能力不足和缺少奖励机制限制了用户的参与度。反恶意软件生态需要广大用户的参与，需要有简单易用和连贯透明的上报反馈机制，奖励为反恶意软件做出贡献的用户，以力求增加用户的参与度。

4.4.2 反恶意软件区块链解决方案（休伯特）

(1) 休伯特的价值主张

针对以上痛点，百度提出了基于区块链技术的解决方案-休伯特。休伯特的价值主张是构建一个全新的反恶意软件社区。以区块链技术结合反恶意软件技术，打造公平开放、价值对等的防治恶意软件安全社区生态。对软件生命周期进行全程溯源，提升反恶意软件的检测时效，缩短滞后时间、减少对合法文件的错误检测，提升对高级恶意软件 APT 的检测能力。让生态中的各个软件公司、安全厂商、分发渠道、终端厂商，个人用户、政府用户、企业用户等均能受益。提升我国与其他国家在恶意软件攻防方面的对抗能力。

(2) 休伯特与区块链技术的结合点

基于区块链技术的自治性特点，构建数据上链后，由社区成员共同记录、鉴定、广播、溯源的实时防治机制。形成全流程、快速打击恶意软件的新态势。

基于区块链技术的不可篡改性和共识机制，数据被链上成员一致和有效的识别，个体无法私密的篡改记录，避免对合法文件的错误检测和攻防行为。

基于区块链技术的去中心化和开放性特点，打破封闭的旧模式，开放数据共享，以贡献多获得多为原则，将成员和用户的贡献和消耗永久写入区块链。利用积分作为纽带，贯通反馈和响应链条，分散节点，共享账本，打造高可靠、高可信、高价值的社区。实现社区成员和用户的互动，提升反恶意软件生态中用户的参与度，助力提升行业效率。

（3） 休伯特的优势

- 1) 数据优势：休伯特基于百度安全的反恶意软件产品，服务了多种百度旗下软件，如百度App，百度网盘，百度海外产品等，及数十家分发渠道和多个终端厂商。每日处理的软件安全检测达亿次级别，有着庞大的数据优势；
- 2) 技术优势：休伯特基于百度自主研发的反恶意软件引擎，其已将云计算、大数据和深度学习神经网络技术结合，应用到百度安全产品和服务中，代表了顶尖的反恶意软件技术水平。休伯特依托百度区块链技术优势，有着丰富的模块化解决能力、强大的网络吞吐能力以及高并发的处理能力，以此成为更具公信力的自治区块链体系；
- 3) 品牌优势：百度安全拥有十余年实战经验，依托人工智能和大数据，面向企业和个人用户，有着更加智能、先进的安全解决方案。已联合了70多家终端厂商、安全厂商、高校专家和科研机构的力量，共同解决新时代面临的各种安全问题和挑战。

4.4.3 休伯特未来的发展规划

在今年，休伯特计划联合软件公司、安全厂商、分发渠道、手机厂商、IoT 厂商等共建反恶意软件区块链，打造休伯特社区生态。2019 年，将进一步对个人用户发布客户端，为个人用户提供多种服务，提升开放程度；对政府用户、企业用户发布客户端，解决机构中的安全问题。逐步发展成为新一代反恶意软件生态，在与恶意软件的不断战斗中成为中坚力量。

4.5 个体信息管理

区块链由于其唯一性、防篡改性、可追溯性，非常适合于个人信息的持久保存、管理，以及与其他机构之间的共享。这里重点讨论个体教育信息的管理问题。

4.5.1 个体教育信息管理领域的痛点

(1) 个体教育信息不完整

个体的教育经历相关信息主要有两个应用场景：升学和求职。然而现阶段，从 K12 教育、大学教育、成人教育，到在线教育等各阶段教育信息均孤立地存储于提供相应教育的主体单位信息库内，用户难以系统、全面的获取与自己相关的信息，导致学习者教育信息的碎片化。

在升学场景中，非学历学习经历等与综合素质息息相关的信息难以应用在 K12 教育之后的高中升学、乃至留学申请中。

在求职场景中，由于信息的割裂存在以及持有信息主体对于信息的垄断，导致个人的受教育信息在教育机构间与在用人单位之间的流转极为不畅，直接导致用人单位无法全面核实候选人的背景信息。

(2) 个体教育信息不真实

由于教育信息割裂存在和共享不畅问题的存在，求职人员对教育信息进行作假的成本较低且风险较小，直接导致当下求职人员简历造假现象频发，成为招聘市场较大成本支出的因素之一，亟待得到有效解决。

(3) 非学历教育无成熟认证体系

非学历、终生教育的形式更加多样化。现阶段，线上线下的非学历教育成果认证与进一步转化为就业资本之间仍存在较大的鸿沟，从另一维度上限制了非学历教育用户接受度发展的速度。

4.5.2 个人教育信息的区块链解决方案（百度会学）

(1) 项目背景

目前百度教育事业部旗下产品百度会学，主要是希望通过为优质教育资源的聚合、严选，为用户提供个性化的教育资源和服务，帮助用户实现升学、就业等目标。



图 17 百度会学首页

通过持续的用户交互、资源（课程、活动、内容、服务等）引入、数据累积，让百度会学成为用户学习、成长过程中闭环的解决方案。百度会学目前实现了海量网络教育资源的汇聚和评价，下一步将会联合头部机构打造闭环服务，通过联合垂直领域的头部机构，共同为学习者提供最优质的教育内容和服务，并通过对学习者的综合能力进行认证，帮助用户实现升学、就业的目标。

这些愿景的底层基础就是真实地记录用户的学习行为及相关成就信息，在信息的流转、共享中，保证信息的真实性以及不可篡改性，以实现最终构建起学校、用人单位、应试人员之间的诚信体系。

（2） 百度教育的区块链解决方案

1) 百度会学区块链解决方案

百度会学利用自身优势及区块链技术提出百度会学区块链解决方案，试图解决现阶段个体教育信息存在的问题。教育区块链项目的愿景是为用户创建一个去中心化的、安全加密的、真实的受教育及工作等信息的升学就业身份证明，力求在 K12 学生的升学、留学以及毕业学生就业场景产生实用价值。一方面，用户学历及非学历教育经历是其升学、实习、就业的真实信息背书；另一方面，可信数据的流转可以省去企业在招聘过程中花费的高额背调成本。

用户信息上链将分为信息初建阶段和信息完善阶段。在信息初建阶段，基于用户授权，结合区块链技术将用户在百度会学及其合作伙伴（各类线上、线下行业头部培训教育平台）的学习成果与用人单位和招聘平台之间进行信用共享，做到学习成果的认证、真实保存以及流转的打通。在信息完善阶段，在用户授权的前提下，

逐步加入用户学历教育信息、工作信息，不断拓展信息维度，使之成为用户的“升学就业身份证明”。

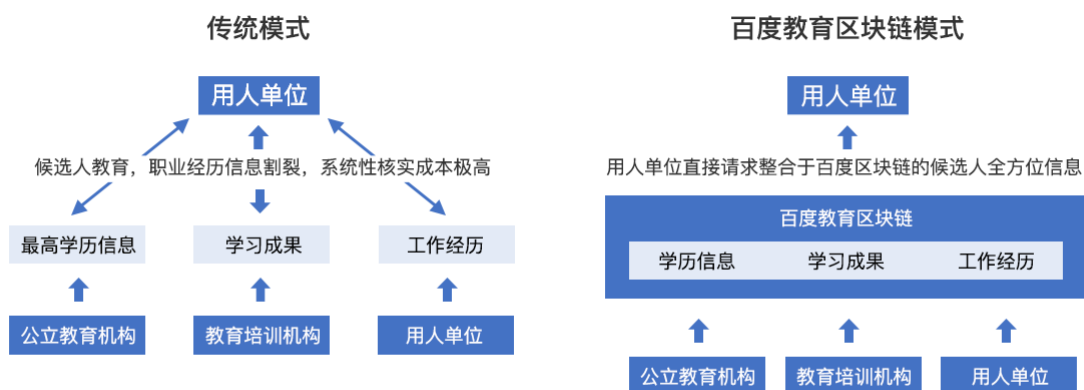


图 18 传统信息核实模式与百度教育区块链信息认证模式对比

2) 百度会学区块链的使用场景举例

① 场景一：用户学习认证

学习者在完成培训学习及认证后，向百度会学区块链平台申请认证上链，信息核实后开通账号，教育平台将认证结果永久存储在百度会学区块链平台。用户在升学、留学、就业等场景可以授权学校、用人单位查询其学习认证的信息。

② 场景二：用人单位核实候选人信息

用人单位欲通过百度会学区块链平台核实候选人简历信息真实性，在获取候选人授权后，用人单位可通过百度会学区块链平台核实候选人的真实信息。

③ 场景三：用人单位协助认证离职员工信息

用人单位可以在两种情况下协助其员工获得职业履历的认证。首先是在员工离职时，可向公司人力申请在百度会学进行职业履历认证上链；其次，用人单位在使用百度会学辅助招聘时，收到离职员工工作履历认证请求后，完成对离职员工的工作信息认证。

④ 场景四：K12 学生升学留学

K12 学生在升学、留学的申请过程中，完成在百度会学区块链的账号开通、学习成果认证后，向目标学校申请时，可通过向目标学校授予权限，允许目标学校查看自身学历、非学历等教育信息。

⑤ 场景五：教师课程成果认证

教师在教育平台完成课程授课并经过一段时间后，课程的学习量、点评量趋于稳定后，教师可向百度会学区块链平台申请开通账号，并完成教学课程成果认证。

(3) 百度会学区块链的产品优势

1) 百度教育的平台优势

百度教育平台拥有品牌、流量及信誉优势，有能力汇聚众多教育平台及国家公立教育机构形成“教育区块链生态联盟”。

2) 技术优势

百度超级区块链，拥有单链 1-10 万 TPS 的超高性能，可支撑百万量级商家和亿级别用户的在线实时匹配和合约处理。

3) 品牌优势

百度搜索是国内最大的搜索引擎，与百度区块链成为合作伙伴可大幅提升自身的行业影响力，在目前在线教育市场竞争白日化阶段，将获得更多的筹码。

4.5.3 百度会学区块链的实现路径

(1) 百度会学区块链联盟的成员架构

百度会学区块链链上接入的成员主要有七类：教育培训机构、高校、政府部门、用人单位、个人用户、招聘平台、百度会学区块链平台。通过各类机构的认证提升百度会学区块链的公信力和背书，打造真实、可信的用户教育信息及就业信息的平台。

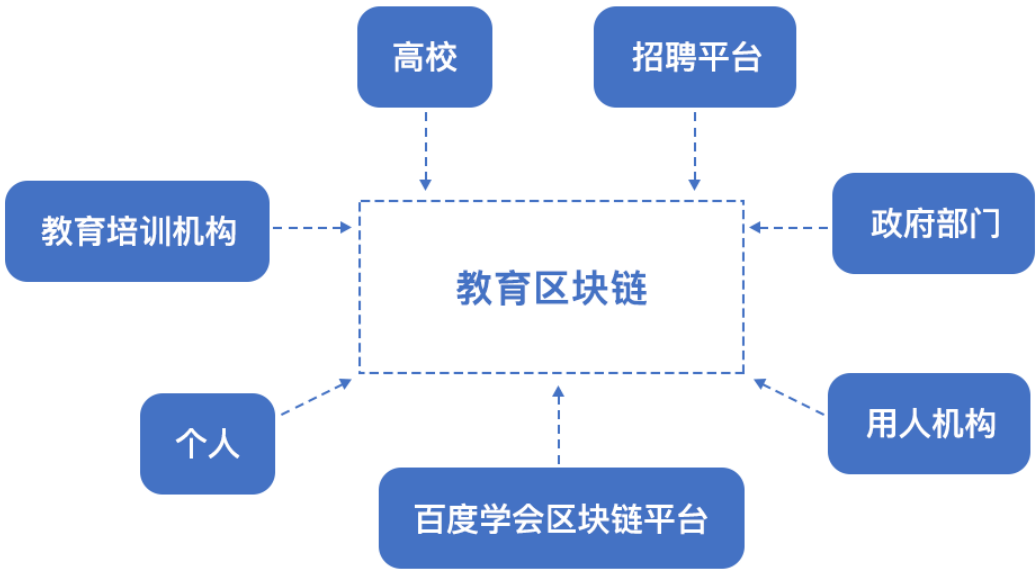


图 19 教育区块链节点成员架构

(2) 百度会学区块链的实现路径

产品实现路径整体分为两个阶段：第一阶段主要为内容及认证阶段，主要完成汇聚全网教育资源、搭建服务、能力测评体系、认证、用户教育信息上链的全流程；第二阶段为就业服务阶段，主要完成在用户授权的前提下将用户教育信息进一步开放给外部需求机构，打造闭环的用户信息流转通路。

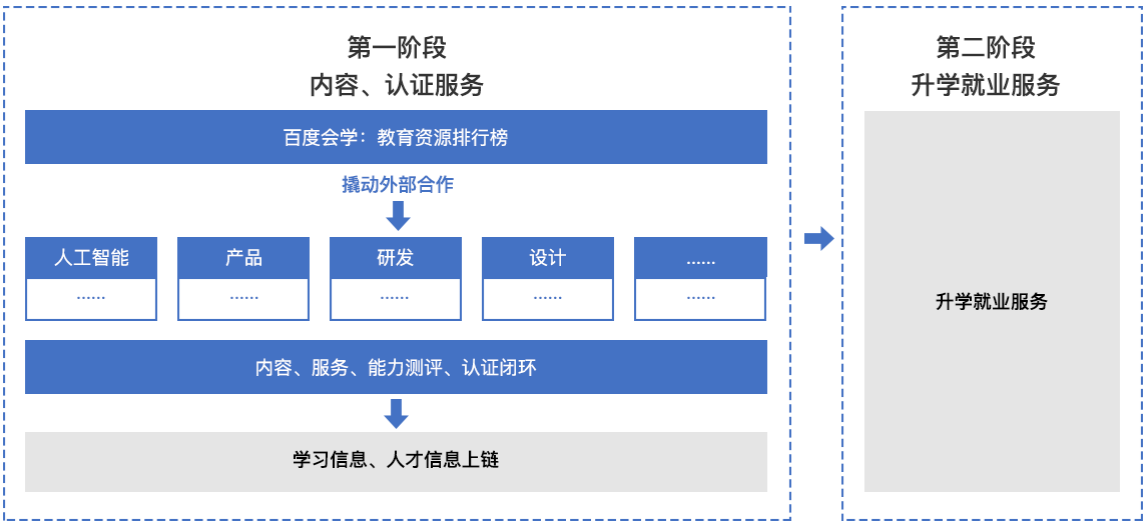


图 20 产品实现路径

4.5.4 百度会学未来的发展规划

最终的愿景是在用户授权的前提下，将用户的学习成果、就业信息上链，打造用户从教育到工作的全方位权威信息库。

首先，与头部非学历教育机构合作，为学习者提供内容并且提供学习成果认证信息上链服务；然后与公立教育机构合作，将学生素质及学历信息上链；最后，与用人单位合作，将员工职业履历信息上链；最终将百度教育区块链打造成为用户的全方位教育、职业信息库，帮助用户在升学、就业场景下更好的实现人生目标。

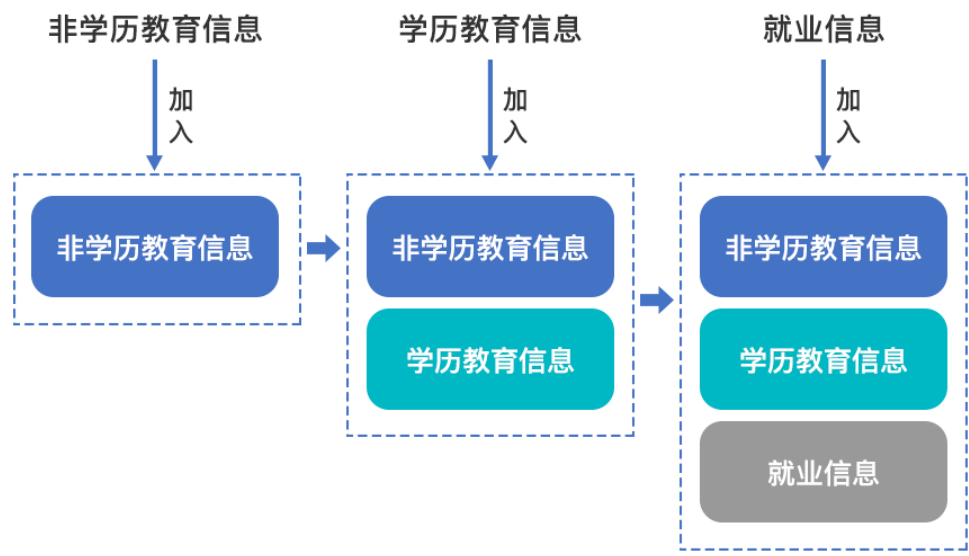


图 21 教育区块链信息库数据纬度

4.6 数字广告

4.6.1 数字广告领域的问题及应对

(1) 数字广告领域的现存问题

随着互联网的普及，数字广告业务已经成为企业非常重要的营销手段，以搜索广告为例，其市场规模正以每年 30%-50%的增速上涨。仅在中国，通用搜索广告市场规模在 2017 年已经达到 600 亿人民币以上。

在通用搜索引擎产品里，用户提交搜索关键词（Query），对引擎返回的结果（包括广告和自然结果）进行自主选择点击跳出到目标落地页。作为用户意图理解能力很强的变现产品，经过多年的迭代，通用搜索广告已经成为互联网广告领域变现效率非常高的方式。

然而，受限于搜索引擎即搜即走的产品模式和用户隐私保护策略，商家对用户意图的理解仅限于用户即时提供的关键词，用户和商家的交互场景仅限于搜索结果列表页。如果能在搜索引擎中扩展用户和商家的交互场景，让商家和用户可以充分利用彼此的信息，将大幅提升商家为用户提供服务的体验，相应地，市场潜力也会显著提升，用户也能获得更多价值。

1) 低交互效率

通用搜索产品追求即搜即走的产品模式，策略迭代以优化用户更短满足路径为目标。用户在搜索引擎结果列表页的停留时间很短，没有在列表页获取位置的商家将完全失去和用户交互的机会。即使获得位置的商家，如果用户没有发生点击转化，商家也很难再获得与用户交互的机会，赢得订单。

从商家的角度来看，用户需求的理解仅限于用户即时搜索的关键词，和用户交互的点仅限于用户点击到落地页后的短暂时间。如果用户没有被商家的创意打动（事实上这个概率高达 95% 以上），商家将失去用户。

一个典型的案例是：在电商领域，电商平台依托强大的账号体系和用户浏览行为，常常会对浏览过特定商品的用户赠送优惠券，激发用户消费。而在搜索产品里，只有当用户再次搜索类似商品时，才可能去展现优惠券信息，激发效率低。

2) 隐私安全限制信息的充分利用

搜索引擎作为一种中心化的产品，出于对用户隐私的保护，即使在用户的商业诉求非常明确的情况下也不会向商家开放用户的行为数据，这是搜索引擎必须遵循的底线，但确实也造成了商家和用户匹配需求的低效，对用户也是潜在的损失。一方面，商家如果知道大量用户有特定意图，比如购买英语培训课程，会制定对应的优惠促销计划（优惠幅度依赖用户量）；另一方面，意图购买英语培训课程的用户，也希望找到促销的优惠信息。如果能为相同意图的商家和用户实现信息传递，将是双赢的。然而，这依赖商家和用户的互信，即商家信任搜索引擎真有足够触发特定优惠的用户量，用户信任提供意图信息给商家可以获得优惠。

在现有中心化的搜索引擎形态下，因无法建立商家和用户的互信，搜索引擎采取保守策略，屏蔽了商家和用户的信息交互。我们需要去尝试一种去中心化的方式，在保护用户隐私的情况下，实现商家和用户的天然互信，使信息有效流通，实现商家和用户的双赢。区块链技术的引入，无疑是解决这一问题的理想方案。

4.6.2 通用搜索广告的区块链解决方案（百宝箱）

（1） 百宝箱的价值主张

百宝箱的价值主张是构建附着于通用搜索引擎之上的全新商业平台，以百度自研的超级区块链技术作为底层支撑，在保证用户隐私完全安全的原则下做到透明开放，为商家和用户去中心化的商业服务和高效率意图匹配能力，让商家以智能合约的形式发布优惠信息更便捷地找到自己的目标用户，让用户找到合适服务的同时享受到好的优惠，实现通用搜索引擎价值的更大化。

（2） 百宝箱的产品优势

1) 品牌优势

凤巢作为全中国顶尖的通用搜索广告平台，有 10 年以上的商家服务经验，从覆盖广度和服务深度上具有先天品牌优势，可以为用户提供全行业的商品和服务解决方案。

2) 技术优势

百度超级区块链，单链可以实现高达 1 万-10 万 TPS 的吞吐量，目前可以支撑百万量级商家和亿级用户的在线实时意图匹配和合约处理的系统。

3) 流量优势

百度搜索，是用户表达诉求的非常直接的入口，依托现有搜索平台，为用户提供满足意图与诉求的搜索结果之外的延展结果，有着极其自然的使用场景和流量优势。

（3） 解决方案

结合百度超级链的隐私保护、智能合约、通证激励机制等核心功能，建立去中心化的用户和商家直连网络。平台以通证的形式激励用户在网络中表达服务需求，商家以智能合约的形式发布服务能力，用户可以用通证兑换智能合约中提供的优惠，实现平台获

得更多信息、商家获得更多流量、用户获得更多优惠的三方共赢。从而解决了传统中心化搜索引擎无法避免的交互效率和隐私保护问题，实现更高的系统效率。具体方案如下：

- 1) 推出基于搜索的区块链应用百宝箱，作为用户和区块链网络交互的工具。百宝箱以通证激励的方式鼓励用户主动授权行为共享（搜索、浏览等），实现信息的尽可能大流通，提升整体效率，同时借助区块链天然的隐私保护能力保证用户数据的安全；
- 2) 商家利用基于百度超级链的百宝箱提供的智能合约功能发布服务能力，比如“如果过去 3 天内搜索过少儿英语培训的用户达到 100 位，为每位用户提供一张价值 1000 的英语培训优惠券”。平台执行智能合约，帮助商家触达即时搜索之外的用户，扩展了商家可利用的流量；
- 3) 对用户来说，用户搜索意图的满足不再局限于即时返回的搜索结果，通过智能合约达成后的 push 信息、自主调起等方式，实现基于优惠券的延迟满足。

在围绕百宝箱的区块链场景下，引入区块链作为一个天然互信的平台，在提供给用户足够的隐私保护的前提下，将搜索数据上链，实现用户与商户直连。商家可以信赖平台存量用户的数量和质量真实可靠，基于可靠的数据制定合适的促销计划，并以智能合约的方式发布实施。用户在平台上可以找到更优惠的服务，而愿意提供更多有效信息使得平台的意图匹配更精准，提升系统的整体效率。

4.6.3 百宝箱未来的发展规划

百宝箱预期在 2018 年发布并接入百度搜索商业生态，推出百宝箱蓝钻，为用户登录授权和搜索行为上链提供百宝箱蓝钻奖励，并引入优质测试客户发布智能合约实现百宝箱蓝钻和优惠券的兑换功能。2019 年，百宝箱将全面接入百度智能小程序生态，用户使用百度智能小程序（资讯阅读、游戏试玩、服务试用）可以获取百宝箱蓝钻，并兑换小程序内权益完善百宝箱功能，持续扩大百宝箱的用户量，并开放智能合约给教育、电商、游戏、金融、本地服务等行业商家。

未来与展望

区块链技术正处在高速发展的时期，它以颠覆传统技术的独有优势，让我们有理由相信区块链将对现有经济社会产生巨大影响，有望重塑人类互联网活动形态，进而改变社会生产关系。一个鲜活的、充满朝气的区块链可编程社会向我们扑面而来。

百度一直走在高新技术的最前沿，坚持打造联盟生态，与联盟成员共同搭建政产学研平台，推动区块链核心基础技术研究，构建可信区块链标准体系，促进区块链应用落地，引导行业良性健康发展。

百度将进一步推进超级链的社会化部署，百度自身仅作为节点参与其中，一起为超级链提供公信力。由于超级链网络正处于起步阶段，需要有百度这样的技术强者领军，慢慢做大做强。

超级链除了支持百度现有业务以外，也将全面支持共享经济下的新型产业结构。百度计划联合业界翘楚和地方机构，成立区块链产业基金和区块链孵化基地，对 DApp 开发者在各方面资源投入都有一定的支持和倾斜。

百度将重点赋能、支持利用区块链技术解决食品安全、商品质量、新零售、新制造、供应链金融、知识产权保护和交易、出行、旅游、社交和游戏等领域的项目，响应国家共享经济新模式的大方针和指导方向。

百舸争流、百花齐放。积蓄了钻研多年的技术能量和多场景运用的宝贵实践经验的百度区块链诚挚邀请生态伙伴加入，发挥区块链技术的正能量，更好的服务于实体经济和用户。百度区块链将开放超级链（XuperChain）生态，提供底层的基础支持和开发者工具，让企业和个人开发者专注于应用创新和功能开发，以协助开发者快速创建区块链应用，或轻松将业务上链落地。

中国日新月异的网络信息技术，已经深度融入社会生活的方方面面。区块链、人工智能、物联网、大数据、云计算等新技术、产品和模式也不断涌现，一批技术已经进入国际市场第一方阵。

百度区块链实验室，希望集众家之所长，合众人之智慧，不忘初心，潜心研究和实践前沿核心基础技术，让技术成果更好的造福人类。



超级链官网



超级链微信公众号

