

腾讯云区块链TBaaS 产品白皮书

2018年3月



发布：腾讯云、腾讯研究院、腾讯TEG计费平台部、
腾讯“互联网+”创新研究中心、腾讯开源



前言

每一次产业变革的浪潮都带给世界全新的机遇与想象。

区块链技术的诞生，真正意义上为数字经济提供了全新的价值转移通道，其应用场景几乎不可限量。工信部于2016年正式发布的《中国区块链技术和应用发展白皮书》，充分展示了国家层面对区块链技术的重视程度。

然而，目前区块链底层技术不完全成熟、基础设施未全面完善的形势还没有获得根本性转变，企业无法快速地投入生产力到基于区块链技术的各种业务场景中去，区块链技术面临的普及性问题亟待解决，值此关键时间窗口，腾讯云区块链（TBaaS）破茧而生。

2015年3月，“互联网+”战略被写入政府工作报告成为国家级战略，腾讯坚持做互联网连接器的定位，完全契合国家层面的指引方针。腾讯云区块链（TBaaS）同样延续了腾讯的战略定位，以降低区块链技术的应用门槛、打造可信赖的企业间价值通道为使命。腾讯云区块链（TBaaS）的推出，将使个人、企业级用户不仅能够便捷、高效、安全地享受到区块链技术的价值，且对其主体业务不会造成任何形式的侵扰，充分体现了“区块链+”的战略定位。

大鹏一日同风起，扶摇直上九万里。体量巨大的市场需求和前景可期的应用场景，将为整个区块链生态的发展提供强大助力。腾讯云自始至终是值得信任的云服务平台，我们热忱期待与行业为伍、与趋势为伴，为企业、个人客户提供更为优质的云服务，带来更为友好的云体验，为云技术、区块链技术的繁荣发展做出应有的贡献。

腾讯云区块链（TBaaS）将是一个有能力为客户创造和提供商业价值的智能服务平台，其以云计算平台为依托，利用区块链技术与各行业应用相互融合，推动自有产业转型升级，为客户创造全新的产品、业务和商业模式。为了充分阐明和体现腾讯云区块链（TBaaS）能够赋予全行业的商业能力，我们编写了本白皮书，主要包含如下内容：

一、阐述了区块链的起源与发展。首先对区块链的技术原理进行了讲解，提出了区块链多方共识、弱中心化、信息不可篡改以及智能合约等特点，并介绍了区块链在社会关系、经济效益等层面所带来的积极意义。

二、对区块链应用领域的介绍。通过援引“区块链+场景”的案例，详细阐述了区块链在金融、供应链、公益慈善、公共服务、物联网、共享经济等相关领域的各类应用。



三、对腾讯云区块链（TBaaS）开发平台的介绍。首先介绍了腾讯云区块链诞生的原因，并对其设计原则进行了详细讲解，然后说明了其能够为行业带来的不同服务能力，最后对其后台技术架构进行了相关介绍。

四、基于腾讯云区块链（TBaaS）的应用场景及解决方案。提出了包括在共享账本、公证与记录、互助保障、数字资产、防伪溯源、物联网、共享经济等应用场景能够解决的业务痛点，并分别枚举了相关案例进行阐述说明。

五、对区块链未来应用的展望。基于现有的区块链应用场景，对区块链的多平台互通、链外信任机制，以及其在未来能够带来的更大价值进行了开放式的展望和创想。

腾讯云区块链团队

2018年3月30日



编写成员

顾问:

卢山、邱跃鹏、王慧星、陈广域、许菁文、司晓、李纲、胡利明

协调与策划:

张绪源、周洪飞、潘安群、常佳、张孝荣、杜晓宇、彭宏洁、邓建威、
金欢、费强、陈宁国、王春雨、吴楠、梁雪

研究撰写:

张绪源、周洪飞、吴非、章贡、李佳、尚志豪、吴楠、李亮、陆曼、
曾首润、陈宁国、刘长辉、杜智超、杨佳、徐禄、王颖涛、司云雷、
温伟力、李叶、周小芳、庞哲维



目 录

1. 区块链起源与发展	8
1.1 区块链技术是什么	9
1.2 区块链的特点	10
1.2.1 多方共识	10
1.2.2 弱中心化	10
1.2.3 信息不可篡改	10
1.2.4 智能合约	10
1.3 区块链的意义	10
2. 区块链应用的领域	12
2.1 金融领域	12
2.1.1 区块链+支付（国际清结算）	12
2.1.2 区块链+保险理赔	12
2.1.3 区块链+交易所	13
2.1.4 区块链+数字资产	13
2.2 供应链领域	13
2.2.1 区块链+物流	13
2.2.2 区块链+溯源防伪	14
2.3 公益慈善领域	14
2.4 公共服务领域	15
2.4.1 区块链+政务与司法	15
2.4.2 区块链+文化与教育	15
2.4.3 区块链+医疗	15
2.5 物联网领域	16
2.6 共享经济领域	16
3. 腾讯云区块链产品介绍	17
3.1 腾讯云区块链概述	17



3.1.1 TBaaS 为何做联盟链	19
3.1.2 TBaaS 的设计原则	19
1) 开放性	19
2) 高可用性	19
3) 极致性能	19
4) 自动化部署	20
5) 智能监控	20
6) 高性价比	20
7) 全球互联	20
3.1.3 TBaaS 的服务能力	21
3.1.4 TBaaS 的技术架构	22
3.2 TBaaS 产品特色	23
3.2.1 云上服务	23
3.2.2 私有云服务	24
3.2.3 隐私保护	24
3.2.4 多链支持	25
3.2.5 合约管理	26
3.2.6 共识机制	28
3.2.7 开放机制	28
3.2.8 证书管理	28
3.2.9 硬件加密	28
3.2.10 按需存储	28
3.2.11 企业互联	29
3.2.12 网络管理	30
3.2.13 策略和权限管理	31
3.2.14 账号管理	31
4. 腾讯云区块链应用场景与解决方案概览	32
4.1 共享账本	33
业务场景	33



解决的业务痛点	33
应用案例1：保险理赔	33
应用案例2：跨境汇款	37
4.2 公证与记录	38
业务场景	38
解决的业务痛点	38
应用案例：供应链金融	38
4.3 众筹领域	39
业务场景	39
解决的业务痛点	39
应用案例：保险	40
4.4 数字资产	42
业务场景	42
解决的业务痛点	42
应用案例：预付费卡	42
4.5 防伪溯源	43
业务场景	43
解决的业务痛点	43
应用案例1：农产品溯源	43
应用案例2：微信智慧医院处方安全流转平台	45
4.6 物联网	46
业务场景	46
解决的业务痛点	46
应用案例：智能制造	46
4.7 共享经济	49
业务场景	49
解决的业务痛点	49
案例：智能电网	49



5. 未来展望	52
5.1 多种平台支持——让客户更专注于自身业务	52
5.2 链外信任——通往现实世界的桥梁	53
5.3 引领未来——用开放的心态拥抱未来	53
6. 参考文献	54



1. 区块链起源与发展

上世纪下半叶互联网的飞速发展，让人们在信息互联探索的道路上越发成熟，一封电子邮件转瞬就可以环游全球，一张美丽的风景照片很快就可以分享给全世界。可以看到，互联网发展至今，每一项新技术的诞生都在深刻改变着人们的生活方式。如今，一个冉冉升起的新技术——区块链(Blockchain)，来到历史舞台前沿，它让全世界范围内任何一笔比特币(Bitcoin)资产交易在短时间内就可以成功确认。不仅仅是信息的互联，区块链技术帮助实现了价值的互联，这使得越来越多的人关注到区块链技术，了解其原理并应用实践。

区块链(Blockchain)源于两个标志性事件：

- 1) 2008年11月Satoshi Nakamoto（中本聪）发布的一篇论文《Bitcoin: A Peer-to-Peer Electronic Cash System》，翻译名为《比特币：一种点对点的电子现金系统》；
- 2) 2009年1月3日，中本聪公布比特币系统的第一个区块——创世区块，世界上第一个区块链数据诞生。

而后，2013年，程序员Vitalik Buterin受比特币启发后提出以太坊的概念(Ethereum)，并在2014年成立基金会开始发展。发展至今，比特币和以太坊已成为互联网上规模最大的区块链项目。区块链技术也被逐渐应用于各个领域。

在国际上，全球已经有超过24个国家投资区块链技术，80%的银行已启动区块链项目，90多个中央银行加入了区块链讨论，上百家公司加入了区块链联盟。在过去三年里，区块链的风险投资超过了14亿美元，产生了2500+的区块链相关专利。

在国内，2016年底，“区块链”首度被写入《“十三五”国家信息化规划》，中国已有105家区块链相关企业；2017年6月，《中国金融业信息技术“十三五”发展规划》中指出，央行将积极推动区块链和人工智能等新技术的发展。



1.1 区块链技术是什么

比特币和以太坊其底层所使用的链式或者有向无环图（DAG）形式数据存储结构、配套的共识算法、P2P分布式互联技术、博弈论设计思想和密码学技术组合起来被称之为区块链技术。

近年来区块链技术得到了广泛的研究和创新，比特币和以太坊这类任何人都可以参与的匿名开放式共享账本被称之为公有链，而在准入受控的环境下，由多个企业或个人参与运行和记账的区块链平台则是联盟链。二者在共识机制、节点准入、交易性能、激励机制上均有明显的区别，虽然区块链技术源于比特币，但不能将比特币技术所使用底层技术等与区块链技术直接划等号。

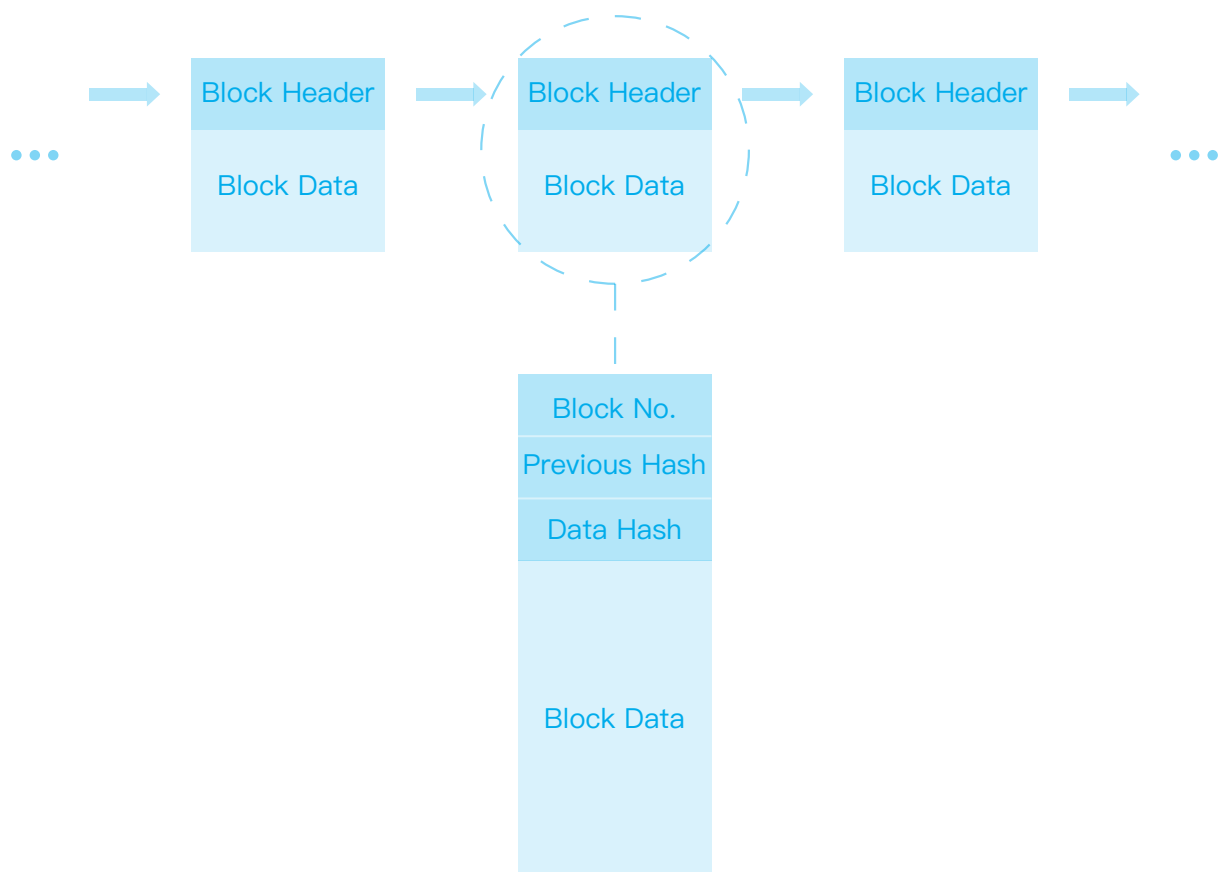


图1-1 区块链账本结构示意图



1.2 区块链的特点

1.2.1 多方共识

区块链作为一个多方参与维护的分布式账本系统，参与方需要约定数据校验、写入和冲突解决的规则，这被称之为共识算法。比特币和以太坊作为公有链当前采用的是工作量证明算法（PoW），应用于联盟链领域的共识算法则应该更加灵活多样，贴近业务需求本身。

1.2.2 弱中心化

区块链网络通常由数量众多的节点组成，根据需求不同会由一部分节点或者全部节点承担账本数据维护工作，少量节点的离线或者功能丧失并不会影响整体系统的运行。

1.2.3 信息不可篡改

区块链系统中所记录的重要信息，均被摘要算法所覆盖，链越长对信息的确认次数越多，且所有参与记账的节点均会存储一份数据拷贝。少量节点对数据的篡改是不被承认的，也无法影响系统整体的运行。

1.2.4 智能合约

区块链系统内部信息不可篡改且所有参与节点均存储账本数据副本，这为智能合约的实现提供了平台。智能合约是区块链技术降低信任成本、颠覆第三方中介机构的有力武器，也是企业使用区块链、实现价值传递和高效协作的工具，同时也是区块链技术实现社会治理的终极价值所在。

1.3 区块链的意义

从技术层面看，区块链技术（Blockchain）并不是一种单一的技术，而是多种技术整合的结果，包括密码学、数学、经济学、网络科学等。这些技术以特定的方式组合在一起，形成了一种新的去中心化数据记录与存储体系，并给存储数据的区块链打上时间戳使其形成一个连续的，前后关联的信任的数据系统。区块链的诞生标志着人类社会开始着眼于打造一个信任的网络。

从经济学层面看，区块链“弱中心化的、分中心化”的特性，并非是让“中心”完全消失，而是其分布式系统弱化了中心的控制。进一步而言，利用区块链技术，以联盟链，私有链或混合链为主，



脱离当前通过制度约束或第三方机构的信用背书，直接实现双方的价值交换，能够有效降低交易成本，提高交易效率，排除交易中人为的干扰因素，从制度上防止任何一方的抵赖。

从社会层面看，与传统工业社会不同，区块链技术创造了一种全新的信任方式，通过技术的实现，使得价值交互过程中人与人之间的信任关系能够转换为人与技术的信任。区块链技术帮助实现弱控制、多中心、自治机制、网络架构和耦合链接等与工业社会完全不同的信息时代的新型的社会结构、商业模式、人际关系。



2. 区块链应用的领域

2.1 金融领域

金融的核心无疑就是“信用”的建立。最原始的商品经济是物物交换，但无疑这样的交易成本非常高，同时还需要面临较高的交易风险。人们意识到这一问题后，很快便过渡到利用信用建立交易的方式，但我们传统的信用建立是需要靠很多强大的背书“中心”的，比如央行、商业银行，以及法院、监管机构等。这就使得传统的交易成本较高，比如去银行贷款，其过程极其复杂且繁琐，经过漫长的审核之后才会决定是否给你贷款。为降低信用建立的成本，互联网金融出现，互联网金融依靠大数据来建立信用，越来越多的互联网金融产品出现，促使信用建立，成本下降已成为时代的趋势。然而，仅靠互联网公司大数据产生“信用”是远远不够的，因为事实上，在当前形势下，大数据必然是每一个互联网公司的绝对内部资源，不可能进行无边的共享，这就产生了“大数据”的多中心的数据孤岛问题。区块链技术公开、不可篡改的属性，为去中心化的信任机制提供了可能，各类金融资产，如股权、债券、票据、保单等均可以整合到区块链上，成为链上数字资产，在区块链上进行存储、转移、交易。区块链，作为金融科技的底层技术架构，必然在很多方面重塑金融业态，在金融领域的应用前景广阔。

2.1.1 区块链+支付（国际清结算）

在支付领域，传统跨境支付与银行间清结算过程中，痛点在于其流程需要经过开户行、央行、境外银行、代理行、清算行等多个机构，每个机构都有自己的账务系统，因此速度慢、效率低。区块链技术的应用有助于降低金融机构间的对账成本及争议解决的成本，同时，使得金融机构能够处理以往因跨境成本而被忽视的小额跨境支付的交易，有助于普惠金融的实现。典型的应用如Visa总部2017年推出基于区块链技术的VisaB2B Connect全新平台，该平台基于区块链创业公司Chain.com的底层平台ChainCore，构建基于区块链的支付统一流程，为金融机构建设处理全球范围内企业对企业交易的基础设施。

2.1.2 区块链+保险理赔

在传统保险业中，保险机构负责资金归集、投资、理赔，往往管理和运营成本较高。需要处理



的理赔单据繁多，处理单据流程时间长，导致时间成本巨大。区块链技术所提供的智能合约的应用，无须投保人申请，也无须保险公司批准，只需要按照智能合约所规定的理赔条件，实现自动核保，保单自动理赔。区块链上数据真实、难以篡改的特点，可有效简化保单理赔处理流程，降低处理成本，降低索赔欺诈的概率。典型的应用案例如2017年腾讯云区块链TBaaS与爱心人寿保险公司共同打造的保险理赔一站式服务。

2.1.3 区块链+交易所

交易所是集中证券交易或商品大宗交易的市场。区块链技术的去中心化、开放性、共享性、匿名性、不可篡改性等特征，可以显著提升交易所登记、发行、交易、转让、交割清算效率，也可以保障信息安全与个人隐私。典型案例如2015年末，全球最大的证券交易所之一的纳斯达克，首次使用了区块链技术交易平台，完成和记录私人证券交易。澳洲交易所利用区块链技术与银行账户链接，买卖股票后资金可以迅速到账。目前在证券界，区块链技术的应用仅在证券发行和资金清算环节，有理由相信，未来区块链技术在各种产权交易中必定会发挥更大的作用。

2.1.4 区块链+数字资产

在金融业务典型的大数据交易、资产交易、共享经济和积分流通与通兑的场景下，区块链技术所提供价值流通能力，能够让区块链帮助在数字资产发行与流通中，实现资产确权、交易确认、记账、对账和清算；而区块链技术的防篡改能力，将有效防止数据篡改，规避内部作弊风险。

2.2 供应链领域

供应链是一个商流、物流、信息流、资金流所共同组成的，并将行业内的供应商、制造商、分销商（零售商、批发商）、终端用户串联在一起的复杂网链结构。而区块链技术作为一种大规模的协作工具，与生俱来地适合运用于供应链领域。

2.2.1 区块链+物流

在物流过程中，利用数字签名和公私钥加解密机制，可以充分保证信息安全以及寄、收件人的隐私。区块链技术可以将信息化的商品价值化，资产化，主要是因为区块链技术的所记载的资产不



可更改，不可伪造。而固定了商品的唯一所有权，可以使得所有物流链条中的商品可追溯、可证伪、不可篡改，实现物流商品的资产化。区块链技术保证货物安全，避免快递爆仓丢包，可以优化货物运输路线和日程安排，并且解决物流中小微企业融资难问题。例如，2016年11月初，欧洲最大港口鹿特丹港与荷兰银行、代尔夫特理工大学、荷兰国家应用科学研究院、德斯海姆应用科学大学鲜花交易中心Royal FloraHolland等组成区块链物流研究联盟，探索区块链在物流领域的作用。这是世界首个专门针对物流领域搭建的区块链联盟。

2.2.2 区块链+溯源防伪

目前，繁荣的市场经济领域中，由于社会分工的精细化，不法商贩利用生产-供货-销售-消费各个环节中的漏洞和信息不对称，制造假冒伪劣商品，给国民经济、产品品牌、消费者都带来很大损害。由于传统方式所限，很难通过技术手段来开展产品的溯源和防伪。区块链技术结合物联网、防伪标签、物流跟踪等产品防伪溯源的手段，防范供应链中鱼龙混杂的原材料供给，防范销售渠道中出现的各类假冒伪劣商品。区块链技术的溯源防伪可以应用于医疗药品的溯源，食品的溯源等场景，例如，伦敦的区块链初创企业 Provenance 为企业提供供应链溯源服务，通过在区块链上记录零售供应链上的全流程信息，实现产品材料、原料和产品的起源和历史等信息的检索和追踪。

2.3 公益慈善领域

众筹领域互助保险在传统运作模式下，存在平台方作弊，监管难度大，公益善款与账目不透明等风险，导致公众缺乏信心，信任无法传递。区块链技术将每个交易方变成网络中的一个节点，各个机构的各项资产、产品以数字化的形式在网络中体现，并解决机构互信问题，形成统一的联盟，实现资金流向可追溯，信息公开透明，全网信息共享；同时，基于分布式账簿，防篡改，流程透明可追溯，规避了内部作弊风险。例如，2017年8月，英国的Start Network汇集了42个知名慈善机构，如乐施会（Oxfam），国际关怀组织（Care International）和救助儿童会（Save the Children），与社会企业创业公司Disberse合作，使用区块链追踪资金的流向，以透明迅速的方式减少资金损失并降低资金滥用的风险，使其资助能最大限度地发挥作用，从而对纳税人和受援者负责。



2.4 公共服务领域

2.4.1 区块链+政务与司法

在公共服务领域中，不论是政务流程还是司法流程，都存在公正与记录的流程长，证据鉴定慢，记录存在作假的风险等问题。同时，传统的存证、电子合同票据与用户信息的记录保全过程中，人们的维权成本较高。区块链所具备的防篡改特性可保障智能合约的执行，为智能合约提供运行的平台。在真实业务场景中，区块链技术可以有效地帮助客户解决公证、信息记录与业务流程长，单据繁多和信息作伪与易篡改的问题。例如，西班牙Stampery公司运用区块链技术，帮助司法鉴定、公证、仲裁、审计等权威机构，记录和存证各项法律文件。

2.4.2 区块链+文化与教育

在文化产业中，版权是非常重要的一环，比如音乐娱乐产业中，大到电影剧本，唱片，IP授权，小到一首背景音乐（BGM），甚至是一段素材片段，都会涉及到版权。而在教育领域中，现有的学生信用体系存在不完善、数据的维度局限、缺乏有效的验证手段、搭建流程复杂以及信息不透明易篡改。通过区块链防篡改与可追溯的特性，可对作品进行鉴权，证明文字、视频、音频等作品的存在，保证权属的真实、唯一性。也可帮助记录跨地域、跨院校的学生信息，追踪学生在校园时期的记录，帮助构建良性的学生信用生态体系。例如，国外的PeerTracks和Ujo就是运用区块链技术在文化领域中非常典型的创业公司。

2.4.3 区块链+医疗

2017年国务院《“十三五”深化医药卫生体制改革规划》当中着重提出了，医疗机构应该按照药品通用名开具处方，并主动向患者提供，不得限制处方外流。同时又探索医院门诊多渠道购药模式，患者可凭处方到零售药店购药。推进“互联网+药品流通”推广“网订店取”、“网订店送”等新型配送方式。在这个政策背景下，智慧医院平台电子处方信息流动过程中的的保密性、防篡改、全程可追溯等需求就成为重中之重。区块链技术能够让患者、医院、药企、卫计委（监管方）等多个参与方形成一个互信联盟，同时满足监管和安全的需求。例如，腾讯微信智慧医院就已经通过区块链技术实现处方信息的安全流转。



2.5 物联网领域

物联网（IoT）蓬勃发展的今天，它不仅给个人消费带来变化，还给整个社会发展带来了深刻变化。目前，大型的物联网平台依靠中心化模型控制各个电子设备之间链接与交互，但是在很多场景下，这种方法变得不是那么实际，比如设备进行数据交换时其中的数据真实性和安全性不能得到保障。而分布式物联网平台正好可以解决这一问题。区块链技术可以帮助实现物联网平台的分布式数据存储，交互，保证数据的安全性和可信性，同时可以记录数据交互的信息。区块链在工业设备、智慧交通与智慧城市等等领域都可以有很好的应用，比如在建筑领域，区块链技术创建了一个去中心化的物联网账簿，账簿可以记录和保存所有智能设备间的交互信息。例如，国外创业公司Filament，运用区块链技术将智能设备信息上链，每个设备在公共账簿上拥有唯一身份信息，打造了一个去中心化的物联网平台。

2.6 共享经济领域

谈到共享经济，总会让人想到共享单车/汽车，共享房屋，甚至共享电力等等。目前，共享经济，它还停留在依靠一个公司或一个平台，让交易双方通过这个中心机构达成交易，完成使用权的不断转移与共享。然而，这并不是真正的共享经济，真正的共享经济是不需要任何第三方中介，用户间可以点对点的进行交易。恰好，区块链技术可以解决这个问题，因区块链其自身所拥有的去中心去中介化的特征，传输数据的过程中数据不可篡改且真实可信，它可以帮助创建出一个真正的共享经济。比如，国外目前很流行的房屋租赁平台Airbnb，一旦运用区块链技术，用户们就可以不再通过Airbnb平台租赁房屋，而是用户间可以点对点的进行房屋空间共享。这种共享经济的生态网络，让闲置的资源，比如房屋、汽车、电力和存储等等都可以实现共享，并给所有共享贡献者经济回报，给共享服务接受者成本更低质量更好的服务。这样，共享经济优势才真正显现出来，优化整个社会资源配置和流通，减少资源的不必要浪费，最终实现共享经济。



3. 腾讯云区块链开放平台介绍

腾讯在云存储、分布式计算、高吞吐网络通信、大数据、人工智能、数据安全等方面有多年的积累，腾讯云提供区块链平台的重要目的就是把这些核心技术优势立体化输出，和区块链技术进行有机结合。用户通过腾讯云区块链，可以把最领先的云端技术和区块链技术一起应用到自身的优势业务中，为业务创新带来新的机会。

腾讯云区块链服务TBaaS（Tencent Blockchain as a Service），采用的是联盟链的方式，深耕技术服务，通过定义统一的标准规范，任何企业都可以在TBaaS平台上轻松地构建区块链服务，为各个领域的合作伙伴提供更多的发展空间。

3.1 腾讯云区块链概述

腾讯云区块链TBaaS，以腾讯云为依托，为企业市场提供金融安全级区块链基础设施服务，通过区块链云上的服务，为行业提供安全、可靠、灵活的解决方案。

TBaaS平台系统不仅符合金融级别的安全合规性要求，同时还具备了腾讯云完备的能力，用户在弹性、开放的云平台上能够快速构建自己的IT基础设施和区块链服务。TBaaS腾讯云区块链开放平台在支持Hyperledger¹ Fabric区块链网络技术的同时，也将支持BCOS, TrustSQL, Corda, EEA等不同区块链底层技术，并打通周边技术生态，为用户提供一整套进行区块链开发、测试，快速部署，弹性可控的企业级解决方案。

¹Hyperledger超级账本：Linux基金会主办的开源合作项目，在行业内已取得企业级区块链技术的领先地位。

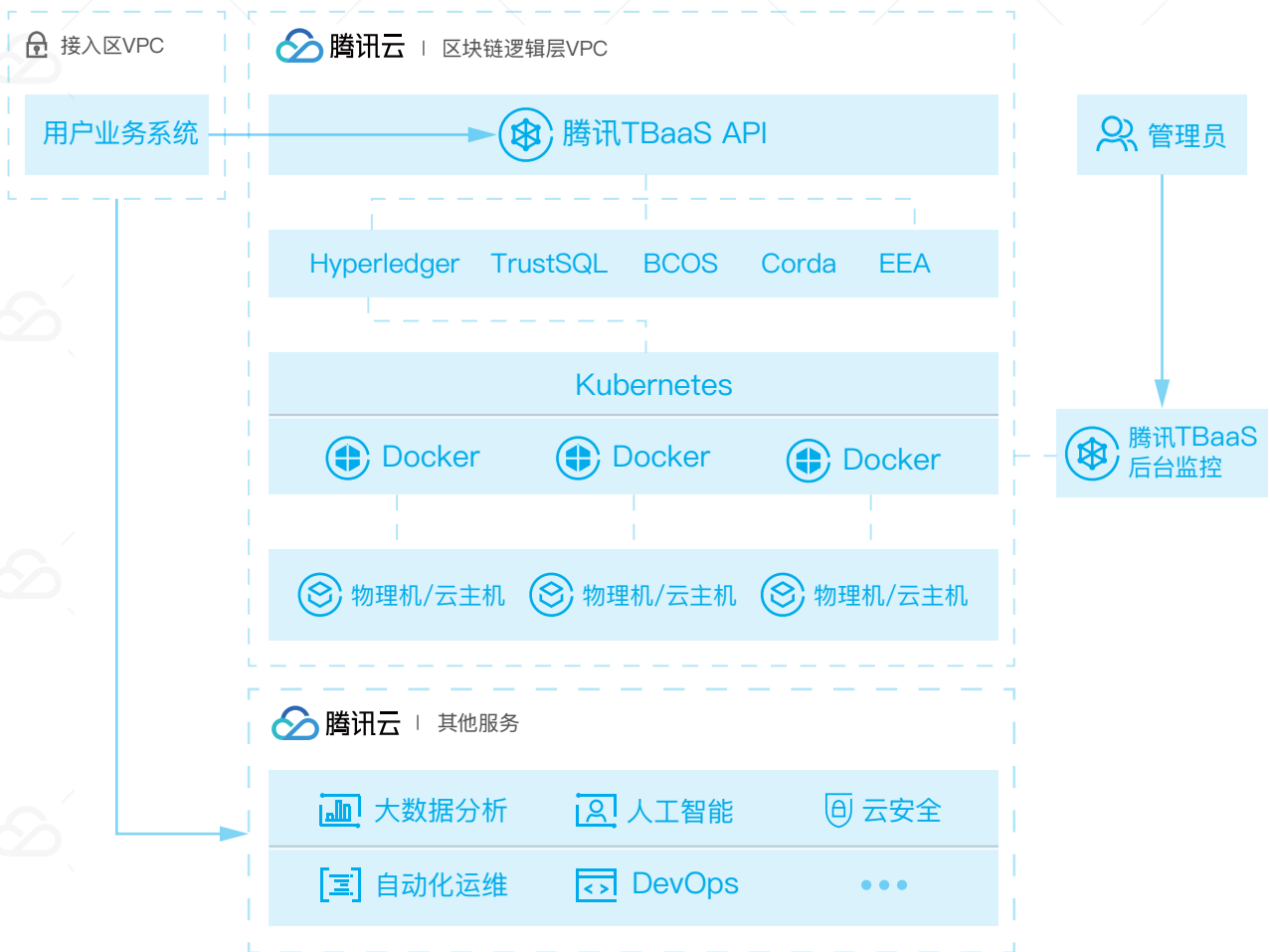


图3-1 腾讯云区块链基础设施架构图



3.1.1 TBaaS为何做联盟链

最早的区块链技术起源于比特币，以比特币、以太坊为代表的众多数字货币技术称之为公有链；而针对企业市场、特别是金融行业，出现了以Linux基金会的开源项目超级账本代表的联盟链。

公有链与联盟链独立发展出了各自不同的技术路径，公有链使用工作量证明(PoW)，即挖矿的方式达成共识并实现数据的防篡改，公有链往往伴随着数字货币/代币作为挖矿的奖励，其基础业务也一般以数字货币的交易为主体；而联盟链针对的是特定的企业或组织，联盟链的加入有一定的准入机制，通过数字证书的方式实现基于PKI的身份管理体系，交易或提案的发起，以参与方共同签名验证来达成共识，因此不需要工作量证明(PoW)，也不存在数字货币/代币，提高了交易达成的效率、节约了大量计算成本(算力硬件投入和电力能源消耗)。

腾讯云区块链TBaaS所做的联盟链平台，顺应时代发展潮流，针对企业市场的需求，开创性的抛弃了数字货币、工作量证明等部分原初区块链技术特性，而保留并发展了分布式账簿、交易共识、数据防篡改等功能。同时，针对企业市场、金融市场的需求又增强了权限管理、安全控制、隐私保护、监督/监管等能力。腾讯云区块链，专注于提供生产级别的、金融级别的安全可信的联盟区块链平台。

3.1.2 TBaaS的设计原则

1) 开放性

- Linux Foundation金牌会员，Hyperledger会员，金链盟会员²，可信区块链会员³
- 源代码开放给Linux社区，提供代码给合作伙伴与监管机构，供对方进行代码安全审查
- 代码兼容社区标准，数据迁移标准化，迁移成本可控

2) 高可用性

- TBaaS 构建于成熟的腾讯云平台，整个平台遵循等保四级高可用设计准则

3) 极致性能

- 开源版本基础上优化平台引擎，单链实现3000+TPS，满足生产系统大吞吐高并发性能需求
- 提供适用商业应用的多链、硬件加密、高性能SSD等解决方案，线性提升TBaaS处理性能
- 多角色节点成员动态加入/退出TBaaS服务

²金链盟：金融区块链合作联盟（深圳）（简称“金链盟”）由深圳市金融科技协会等二十余家金融机构和科技企业共同发起成立。

³可信区块链：在工业和信息化部指导和支持下，由中国信息通信研究院牵头成立的“可信区块链联盟”



4) 自动化部署

- 满足用户个性化需求，一站式快速交付定制TBaaS服务
- 主动升级底层区块链平台和更新补丁
- 多角色节点成员动态加入/退出TBaaS服务

5) 智能监控

- Kubernetes集群7*24监控
- 提供立体化TBaaS平台数据监控、智能化数据分析、实时化故障告警和个性化数据报表配置，实时、精准掌控业务和TBaaS平台健康状况

6) 高性价比

- 可根据用户需求进行弹性伸缩
- 节约运维成本
- 节约监控开发成本
- 按包年或包月的计费模式，减少客户前期投入成本

7) 全球互联

- 拥有62个数据中心，触达全球，助力客户在腾讯云区块链 TBaaS 上跨地域部署
- 领先业界的28线BGP，覆盖国内、外主流运营商

电信 | 联通 | 移动 | 铁通 | 盈通 | 教育网 | 天威 | 长宽 | 互通 | 中信 | 华数 | 鹏博士 | 中联网盟 | 广东广电 | 天津广电 | 中科网 | 东方有线 | 歌华有线 | 方正宽带 | 上海驰联

- Tbps+互联网带宽资源，占全国总流量1/3
- 自建双平面DCI，70Tbps内网互联互通，多机房之间跨域容灾
- 开放态度，接入具备友商云能力
- 全方位网络安全基础能力，包括DDoS防护，入侵监测、漏洞扫描，主机防护等



3.1.3 TBaaS的服务能力

腾讯云区块链服务 TBaaS，是一个企业级的区块链开放平台，可一键式快速部署接入、拥有去中心化信任机制、支持私有链、联盟链或多链，拥有私有化部署与丰富的运维管理等特色能力。TBaaS可广泛应用于金融、医疗、零售、电商、游戏、物联网、物流供应链、公益慈善等行业中，重塑商业模式，提升客户在行业内的影响力。

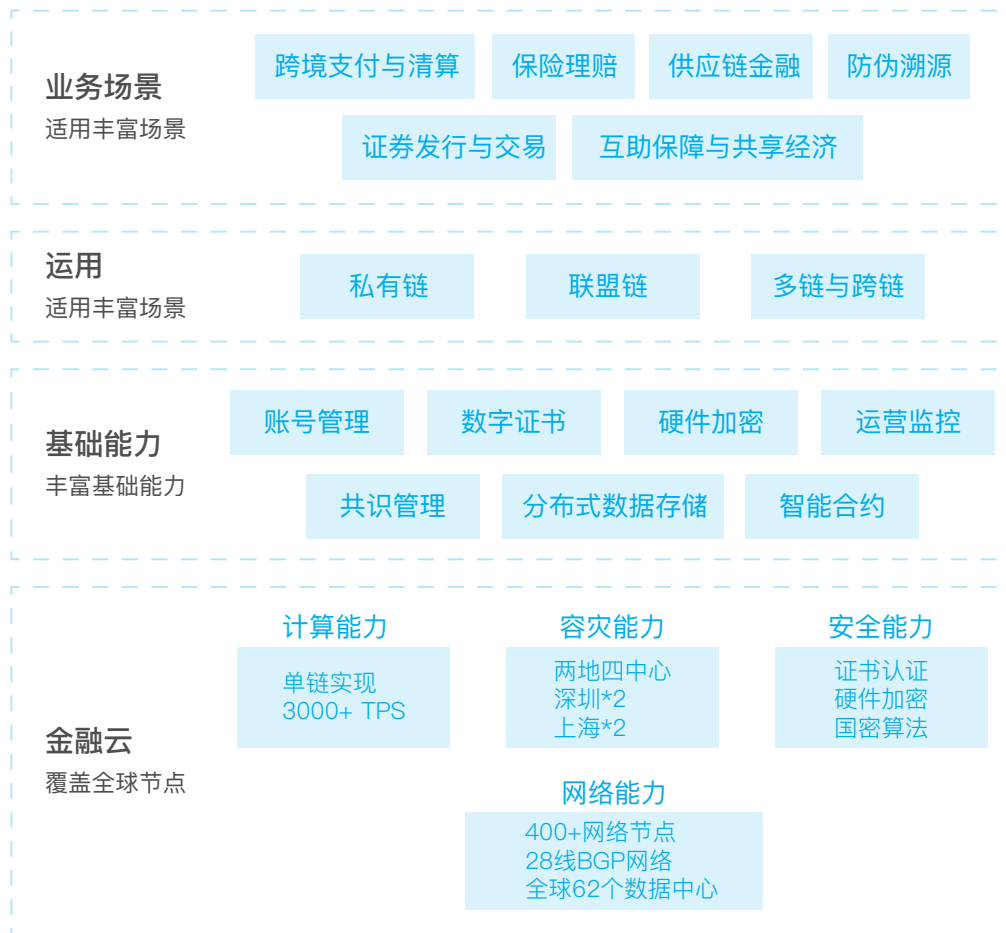


图3-2 腾讯云区块链服务能力



3.1.4 TBaaS的技术架构

腾讯云区块链TBaaS的技术特性有：

- 支持权威CA机构签发数字证书；
- 硬件加速加密/解密；
- 支持国密SM1，SM2，SM3，SM4算法；
- 容器化资源管理，支持多链；
- Devops运维监控；
- 存储系统数据冗余备份，安全可靠；
- 数据迁移标准化；
- 增量恢复技术加快用户数据恢复；
- 冗余物理链路设计，多链路高可靠路径，无单点故障；

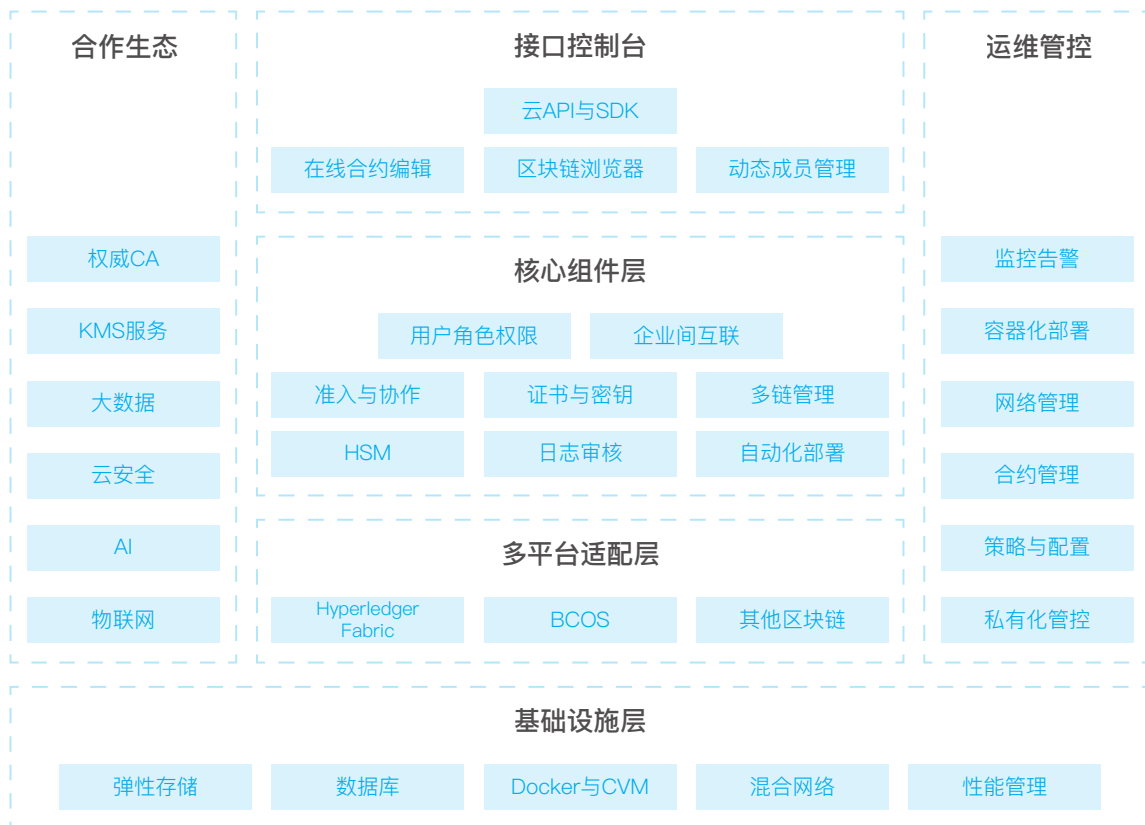


图3-3 腾讯云区块链总体的技术架构图



3.2 TBaaS产品特点

3.2.1 云上服务

TBaaS上为客户所提供的区块链服务，遵循一个联盟一个系统的原则，不同的联盟链(不同的客户)，不仅在逻辑上是严格隔离的，在物理资源（机器硬件、网络、存储...）同样是互相独立的系统，完全符合金融安全监管要求。

只有在同一个联盟链系统中，才会有资源和信息的共享，联盟链有着安全可靠的准入机制，避免敏感信息的泄漏。

TBaaS云服务遵循标准的区块链底层协议搭建，可以兼容网络协议一致的友商云平台。在多云融合的环境中，用户可以按照业务需求搭建真正的跨云平台联盟链，解耦用户与底层技术平台的强依赖性，提升区块链平台自身的可信度。

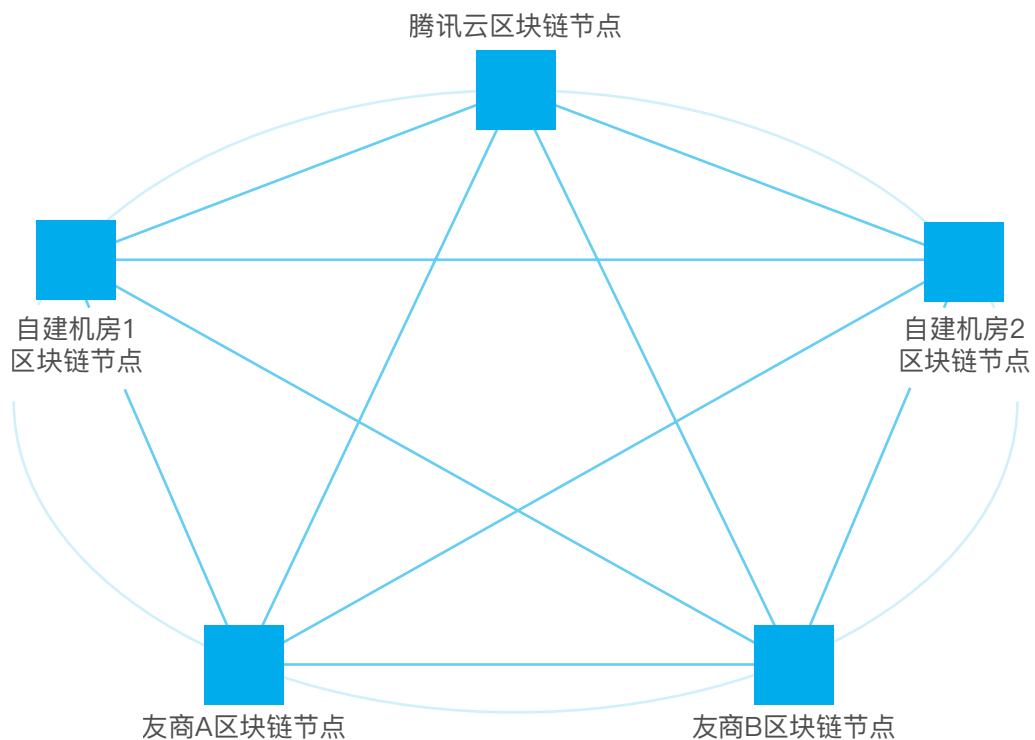


图3-4 区块链节点互联



3.2.2 私有云服务

在金融、电信、政府、能源、教育、交通等行业中，用户的核心业务需要自主可控。为了更好地满足这个诉求，TBaaS支持TCE私有化部署方式。TCE是腾讯云企业级私有云解决方案，经过工信部可信云认证，SLA分别达到99.95%的服务可用性和99.999%的数据可靠性，达到金融行业最高标准级别。TBaaS专有云部署方式搭建在稳健的TCE平台，用户可以自主管控整个TBaaS云平台。

整个私有云构建在微服务治理架构，引入业界优秀口碑Kubernetes进行大规模集群和分布式应用的管理，充分体现Devops持续集成与持续交付的理念。TBaaS服务提供集群和服务两个层级的弹性伸缩能，能够根据业务运行情况，监控容器的CPU、内存、带宽等指标进行自动扩缩服务，同时可以根据容器的部署情况，实现资源的弹性伸缩。TBaaS私有云平台还支持高效部署，修改的业务代码进行快速构建、测试和打包集成，将集成的代码以灰度上线的方式快速部署到预发布环境和现网环境上。

3.2.3 隐私保护

腾讯云区块链平台采用基于数字证书的身份管理、多链隔离、信息加密、智能合约控制等手段保护私密信息。

基于PKI的身份管理：TBaaS平台采用双重身份认证机制，首先通过腾讯云官网帐完成帐号验证；再进入到区块链的权限管理体系，所使用的用户必须通过区块链用户管理中心注册才能获得相应身份证书，只有使用该安全证书签名的客户端节点才能发起交易请求或提案。

- 多链隔离：不同的组织的节点间可以建立不同的逻辑区块链，通过信息隔离，完成不同的组织、不同节点对账簿的隐私保护。账簿在各个组织的节点
- 信息加密：在将数据保存到区块链上之前，可以把数据通过安全的加密方式，将敏感的隐私数据保护起来。另外，也可以将敏感的数据或文件的通过哈希的方式，将其数据指纹保存在区块链上，原始数据或文件以更安全的方式保存。
- 智能合约控制：通过智能合约和访问控制策略来限制访问数据的角色和用户，通过智能合约的方式提供了更灵活的访问权限控制，可以针对节点，针对组织、针对角色、针对用户制定不同的策略。



3.2.4 多链支持

一条逻辑上的区块链是集合了特定组织、特定节点的私有区块链系统，不同的组织间可以建立不同的逻辑区块链，链间实现数据隔离，智能合约可以部署在不同的逻辑区块链之上。

在TBaaS系统中，支持用户在同一个区块链系统中建立多个不同的逻辑区块链，即多链。多链中每一条链都是包含记账节点、共识节点、智能合约和账簿的逻辑结构，它将参与者与数据(包含智能合约)进行隔离，实现了不同角色的用户访问权限不同，数据进行安全控制的基本要求。

多链结构，在不需要增加硬件设备提高成本的前提下，可将热点链拆分为若干并行链，使得数据可以并行写入，提高并行性能。

通过多链的方式进行信息隔离，充分符合用户按照业务场景和参与方建立不同逻辑区块链的实际需求，同时也避免了通讯风暴，节点只在自己的逻辑区块链上进行通讯，提高了效率。

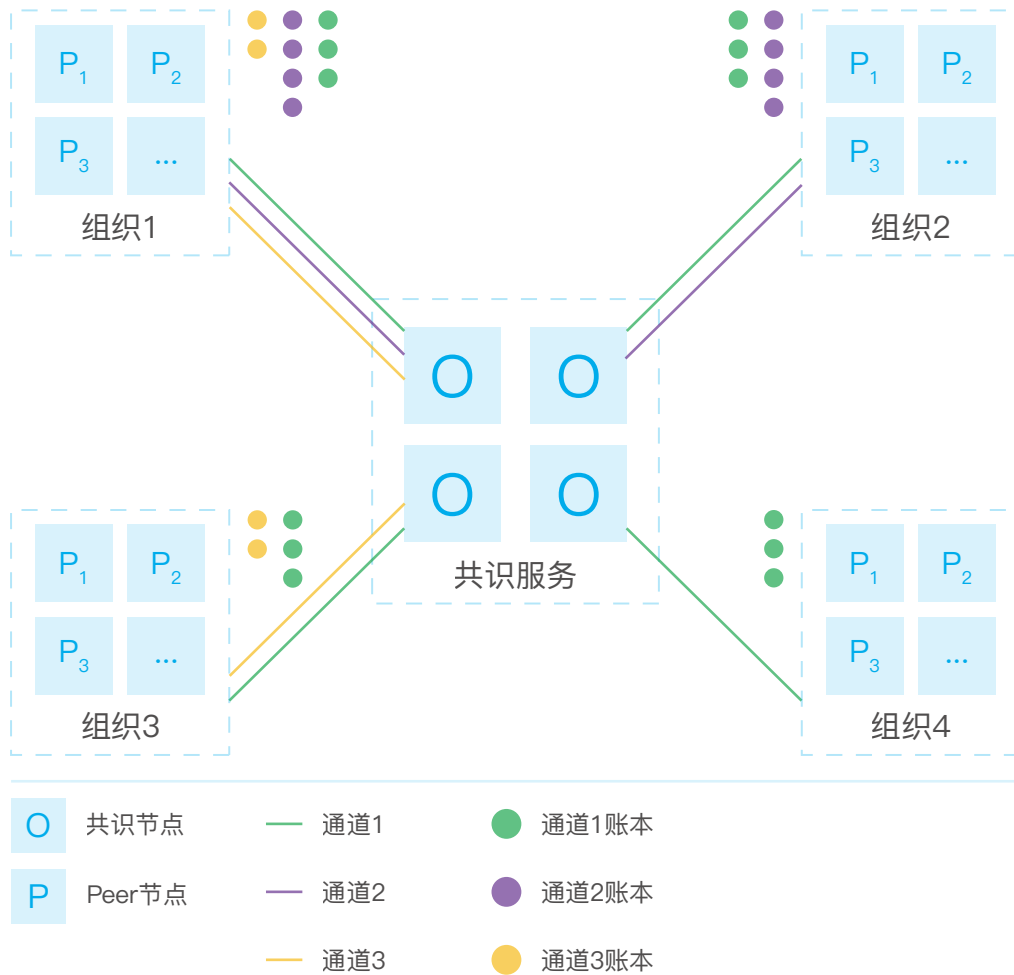


图3-5 Hyperledger Fabric中多链结构图



3.2.5 合约管理

鉴于智能合约开发是区块链应用的主要功能，所有区块链业务能力围绕智能合约为核心，来实现智能合同、自动触发、安全隔离、业务定义、数字协议等功能。因此智能合约是区块链应用开发过程中最主要的部分，客户需要花费大量的精力去编写和调试智能合约。为了解决这一困难，TBaaS平台提供完备的智能合约集成开发调试环境，大大缩短了用户开发周期并减轻了开发压力，以更便捷的方式辅助软件开发。

与其它平台不同，腾讯TBaaS平台不仅可以对智能合约进行词法分析、语法检查，还专门提供了智能合约安全检查服务，对合规性和安全性进行校验，以防止类似于以太坊DAO安全事件的再次发生。

下图为腾讯云区块链即服务的云平台上，智能合约的生命周期示例图：

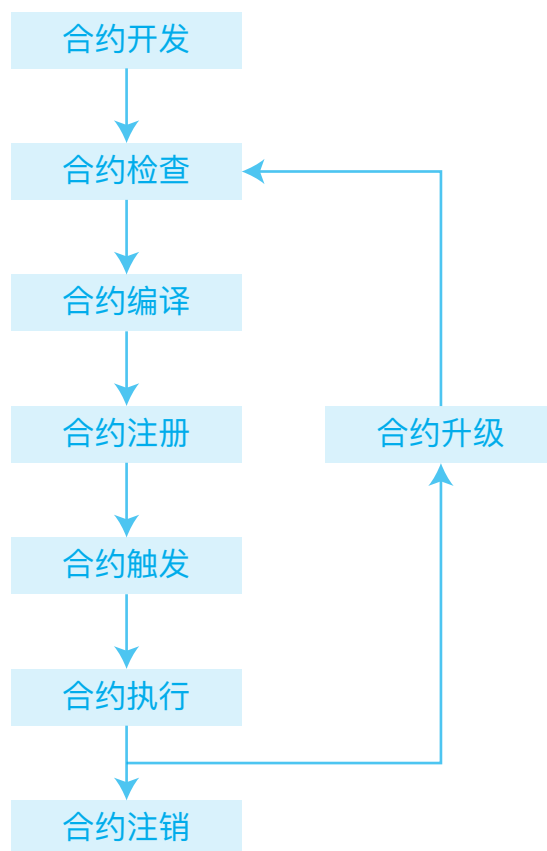


图3-6 智能合约服务



3.2.6 共识机制

共识机制决定了区块链的数据一致性的实现方式和适用场景，腾讯云区块链目前支持超级账本原生共识机制的同时，未来也将支持用户自定义的共识插件和背书插件，方便用户根据自身业务需要进行灵活选择和切换。

3.2.7 开放机制

腾讯云区块链TBaaS是一个开放的服务平台，在支持超级账本Hyperledger Fabric的同时，我们也支持BCOS，TrustSQL等优秀合作伙伴的区块链底层平台，在未来将支持R3 Corda，企业以太坊等区块链等技术，并积极关注区块链前沿科技的发展。

3.2.8 证书管理

与传统的公有链不同，联盟链对用户身份的管理要求和隐私保护要求更高，腾讯云区块链与目前国内领先的证书服务提供商中国金融认证中心（CFCA）进行深度的战略合作，支持在腾讯云区块链中使用CFCA签发企业所需的各类证书，各类证书，用于身份认证、交易监控、交易安全、反欺诈等，为客户带来全平台的证书可识别性和几乎透明的权威CA证书使用体验和一体化的用户与证书管理服务。

3.2.9 硬件加密

腾讯云已具备成熟的硬件加密能力和产品，腾讯云区块链可以直接与其无缝对接，帮助银行、保险、证券等企业充分保护其数据存储安全和传输安全，提升加密解密和签名验签效率，实现密钥安全管理，帮助客户符合监管和等级保护要求。目前腾讯云硬件加密支持绝大部分主流的国密算法和各类国际通用算法，例如SM1，SM2，SM3，SM4，DES，AES，RSA。

3.2.10 按需存储

存储膨胀是当前区块链必然会面临的一个问题，比特币和以太坊当前的全账本数据量已经十分庞大，不适合现今的主流互联网移动端设备进行快速访问处理，区块链在传递信任和价值的代价之一便是消耗了较传统方案多得多的计算和存储资源，如何让存储问题不成为企业上链的隐忧是腾讯云区块链着重探讨的重要课题。一个优秀的存储解决方案应该能不仅需要保证读写性能和数据



高可用性，还应该在中心化集中存储和各节点独立维护一个完整账本之间取得恰当的平衡，帮助企业节省存储成本。云端存储在可扩展性、按量计费、可靠性、可用性、安全性等方面将拥有无可比拟的巨大优势。

区块链在不同场景下的对存储系统要求不同，腾讯云区块链提供了多种存储层解决方案，以适应不同的需求。以Hyperledger Fabric为例，存储分为三部分，账本数据，状态数据和历史数据，账本数据支持使用传统块存储解决方案，例如性能更好的CBS云硬盘或者成本更低，运维更简便的CFS，并支持快照镜像等备份和快速拷贝需求，方便新节点加入区块链后快速同步账本；状态数据和历史数据除了使用原生的GoLevel DB和CouchDB以外，未来可以使用腾讯云端的MongoDB方案。

另外区块链本身毫无疑问也是一个巨大的数据源，目前腾讯云已经支持大数据解决方案与其无缝对接，满足客户在区块链上的大数据需求。

3.2.11 企业互联

云端企业客户通常拥有若干个自己的VPC，VPC之间天然隔离，腾讯云区块链以VPC的形式部署和提供服务，将区块链部署于一个独立的VPC中，不占用用户的VPC配额，同时支持将区块链VPC与其他多个用户的VPC快速打通，不受限于网络地址重叠与繁琐的路由配置等因素的影响，方便用户直接通过自己的VPC访问自己的组织和节点，让客户无需为客户网络互联和后续拓展担心。

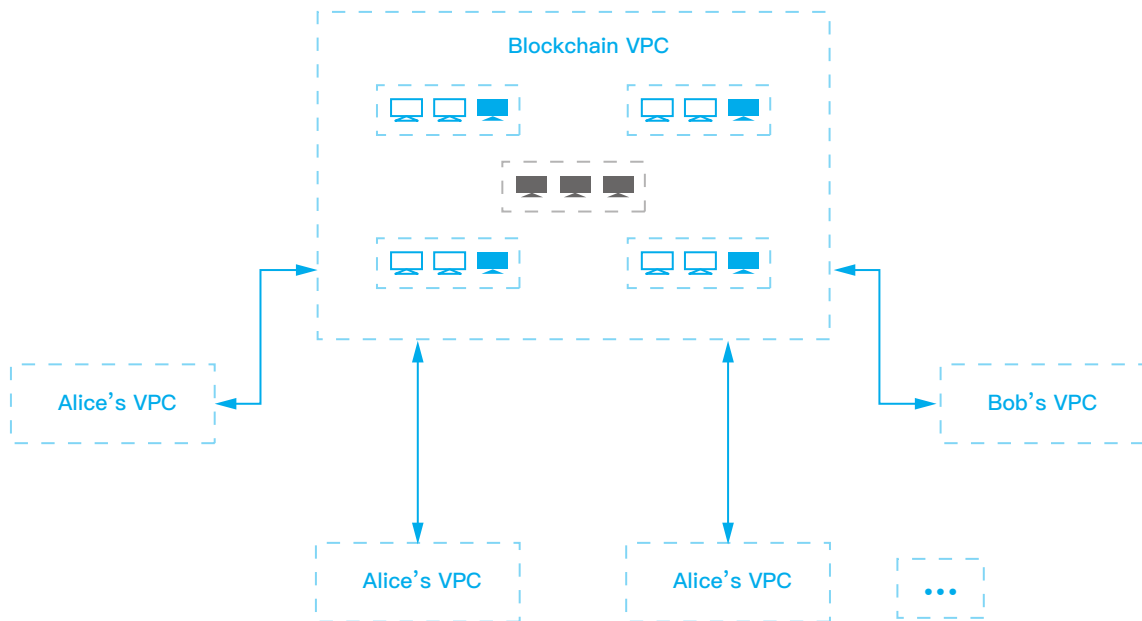


图3-7 区块链VPC互联示意图

除此以外，作为一个开放的平台，腾讯云区块链对用户已有的IT基础设施投资充分保护，能够支持用户复用现有VPC和用户自有IDC内的基础设施，作为区块链的一部分节点。

3.2.12 网络管理

TBaaS平台依托于腾讯云基础设施，提供高速、低延迟的区块链网络，为区块链各个节点间提供无阻塞、无超载的高可靠性的通信，通信保护符合金融级别安全级别标准。

腾讯云区块链的网络遵照联盟链的准入机制，采用多组织联合，区域自治的方式，多链隔离等技术，实现了网络既可以灵活的拓展，又可以实现自适应的管理模式。

- 许可网络：腾讯云区块链网络的成员，首先必须有着经过严格的身份核实，才能加入到某区块链网络，参与方发起申请后需经过组织方的认可才能接入，实现了联盟链的准入机制。
- 区域自治：区块链网络通过不同组织的划分，实现了区域的划分和不同组织的自治管理。组织内部的通信，无需全网广播，而组织之间的通信通过各自的锚节点来进行，既减少了不必要的通信量，又保证了信息的私密性。



3.2.13 策略和权限管理

联盟链仅对成员开放，这种准入机制，以及区块链上的读写权限、参与记账的权限，需要按照联盟的规则来制定。这些机制和规则的集合构成了策略和权限的管理。

权限和策略管理是共识机制的一部分，权限控制的基础是依托于不同策略下达成的共识，策略管理在权限的定义中处于核心地位。策略的制定包含通道策略和共识策略。TBaaS提供了图形化等更加友好的权限和策略方式，帮助客户更好地实现针对不同用户和不同业务逻辑的共识定制。

联盟链针对企业级的管理和监控需求，对用户的权限、角色，和各种共识策略、访问策略进行了全方位的增强。TBaaS为用户提供了完善的管理机制，通过这种灵活的权限策略管理，从而实现了针对不同用户访问权限的控制。

3.2.14 账号管理

腾讯云区块链中，一个组织的帐号分为根帐号和子帐号，根帐号是这个组织的管理员，是组织资源的所有者；子帐号可以有资源创建的权限，默认不拥有所创建资源的权限，子帐号的权限可以控制到单个API接口的粒度。拥有相同功能的多个子帐号可以建组，通过组进行权限管理。

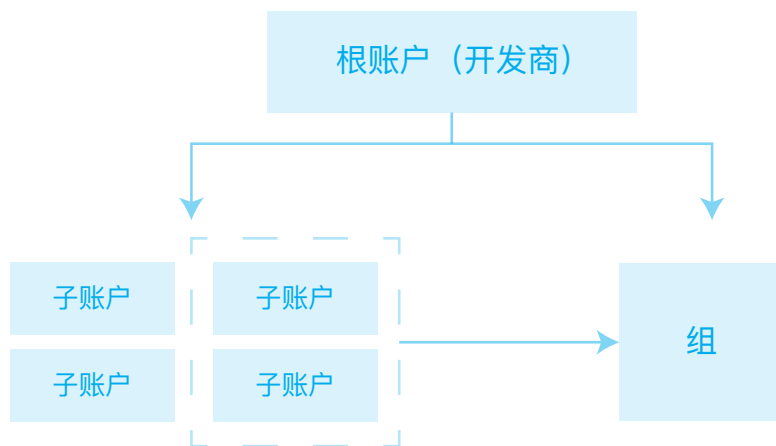


图3-8 腾讯云区块链账号管理

腾讯云区块链的登录体系和敏感操作支持双层安全保护，在用户名和密码之外，再加一层MFA设备，MFA设备可以安装到智能手机等移动设备上。

腾讯云区块链的帐号可以通过邮箱注册，也可以关联QQ、微信等第三方帐号。



4. 腾讯云区块链应用场景与解决方案概览

腾讯云区块链服务TBaaS，专注于用区块链技术应用在不同的业务场景，通俗易懂地帮助用户从业务的角度去理解区块链，并推出特定业务场景下区块链的解决方案。更低门槛更高效地帮助用户方便、快速的构建区块链服务。我们将用户从繁琐、重复性的开发任务中解脱出来，让用户将更多的精力投放在区块链上的服务、业务系统的高级架构设计上。以下为TBaaS为解决用户问题的业务架构示意图：

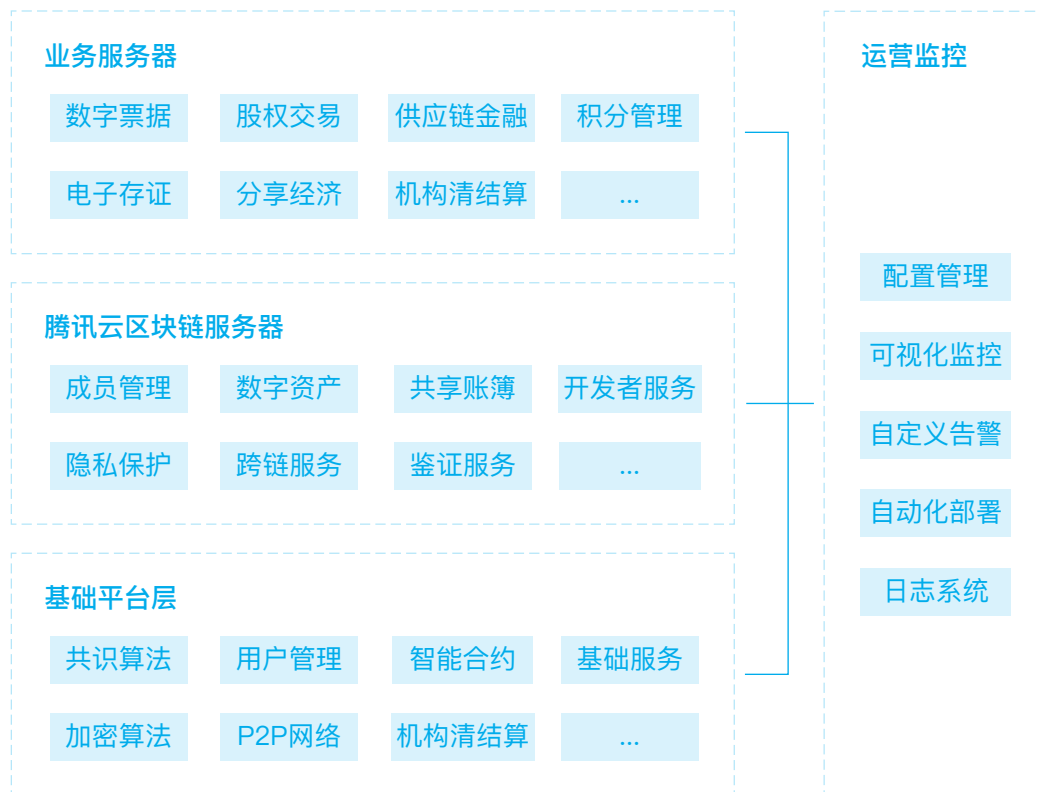


图4-1 腾讯云区块链业务架构图



4.1 共享账本

业务场景

- 1) 快速核保/保险直赔
- 2) 银行间清结算
- 3) 跨境汇款
- 4) 审计

解决的业务痛点

- 1) 保险理赔单据繁多，流程时间长
- 2) 银行间清结算慢
- 3) 跨境汇款时间长，费用高
- 4) 传统审计流程复杂度高，质量与效率受限

应用案例1：保险理赔

传统保险从产品设计到代理人制度销售模式，是一套自上而下的销售管理模式，中间环节繁复，对市场的节奏反馈响应速度慢，不能很好的适应当今快速变革的社会形势。保险业务所面临的挑战和问题，主要集中在以下几点：

- 针对新型的保险业务需求很难及时开拓
- 保险和医疗系统没有打通，理赔的申请、受理、审核及赔付周期长，同时存在骗保的情况
- 保险的生命周期过程（从参保到理赔，最后到赔付）不透明，参保人对保险公司缺乏信任
- 整个保险业务过程都完全依赖人的操作，缺少自动触发和智能控制，因此不仅响应速度慢，而且很难杜绝人为的操作错误、行为疏漏，甚至是恶意篡改
- 信息查询困难，用户很难随时随地的查询自身参保情况
- 再保险业务开展困难，因为缺乏有效的监管机制：防篡改、反欺诈、可追溯
- 传统的保险业务很难做到既要信息公开，又做到隐私保护
- 整个保险业务的IT基础设施建设周期长，成本高，限制了传统保险引入高新科技(大数据分析、人工智能...)，并阻碍传统保险向互联网方向转型



区块链结合保险易用场景，将会革新现有的保险体系。以医疗保险为例，区块链的引入，不仅仅是将数字信息存证保存在区块上，更重要的是：

- 实现信息的共享，在保证隐私的前提下，能够打通保险过程中的各个环节，解决信息不对称的问题，使保险中的流程、上下游机构做到操作、信息的透明
- 实现价值的流通，通过信息共享，为信息的提供方一定的奖励机制，引导医疗系统信息的开放化
- 打通医疗-保险-监管等各个环节，实现真正意义上的医疗与保险业务的电子化
- 通过智能合约来实现保险业务承载于区块链网络中，完成自动核保、智能理赔的高阶目标。而保险的全业务上链后，即可实现业务能力、数据存储的分布式管理，规避了中心化数据中心所带来的一些列问题，大大降低开发及运维成本

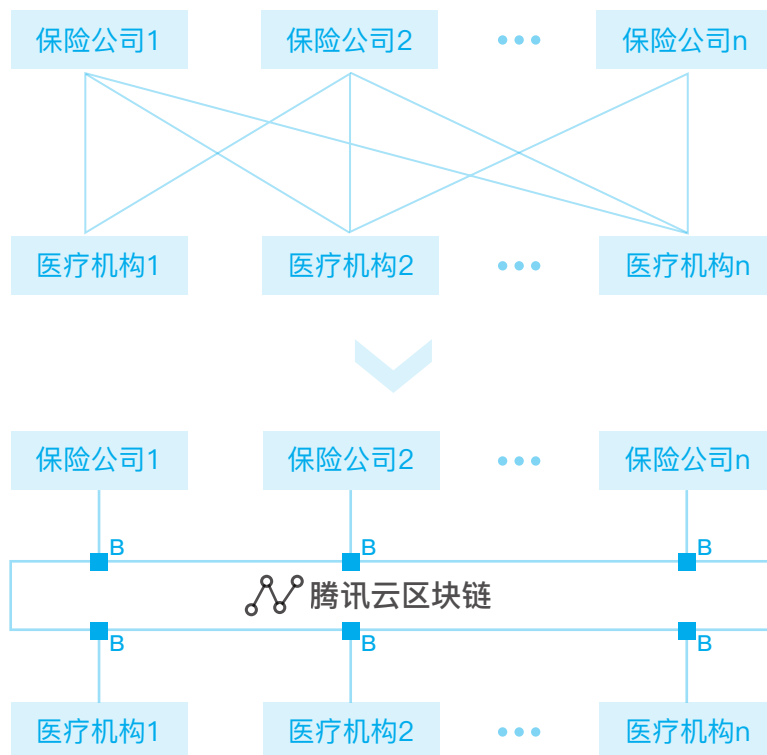


图4-2 引入区块链后产生的变革



区块链系统引入之前，信息的交流模式是零碎的、分散的、无规则的、非通用的、缺乏标准的模式，各个环节需要过去各个机构自身去打通，而各个机构的信息电子化是私有的协议，缺乏统一规范，很难形成统一的共识，这也是目前医疗信息标准化的最大障碍。通过引入区块链，实现了信息的共享，并形成统一的信息交流、通信标准，无需每个机构、每个组织自己去联络并打通。

由于医疗机构自身的封闭性，并且缺乏利益的驱动，导致医疗信息很难共享给体系外的机构。而引入区块链系统后，通过建立起信息和价值交换的体系，最大化的吸引医疗机构将自身的信息开放给保险机构。

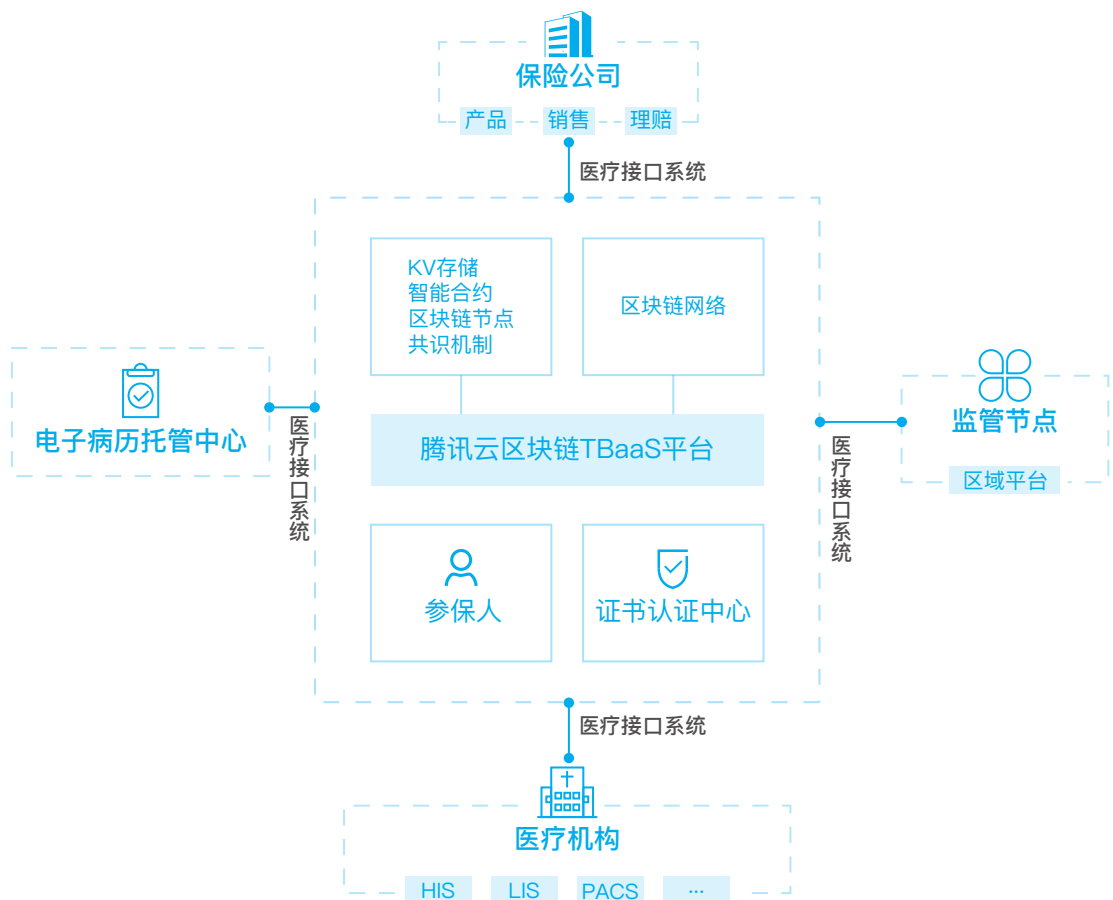


图4-3 医疗保险区块链应用场景



通过智能合约来实现自动核保，智能理赔的过程如下：

1. 参保人在医院就诊后，提出理赔申请，同时将相关就诊信息提交到系统中
2. 提交申请后，自动触发智能合约，系统调用医疗机构接口，对参保人理赔资料进行核对
3. 审核通过后，触发赔付智能合约，保险公司对赔付的钱款进行自动划拨

其中证书中心作为核心节点加入到这个系统中，系统中各种角色，各类节点所使用的电子证书，都由认证中心机构集中管控和颁发。通过引入已经与腾讯战略合作的CFCA(中国金融认证中心)，使得证书的颁发校验更具金融合规性，使得电子存证真正具备法律效应。

同时区块链技术使得再保险的业务能力成为可能。再保险是基于原保险的保险，从根本上讲，是一种“再合约”的过程。区块链将催生“再保险2.0”时代的到来，其重要特征是“风险新分散”，是再保险职能的新存在。共识机制、时间戳和智能合约将扮演重要角色，将给再保险，乃至保险创新以全新的启发和路径。

最后，我们将利用区块链技术建立展示平台，将资金信息、保单信息、会员信息等共享到区块链当中。其中除了涉及到存证能力之外，还有一项非常重要的方面就是治理能力。腾讯云区块链即应用的平台可以引入监管机构、第三方媒体和会员，共同参与平台的监管。我们的平台是一个开放的平台，其业务模式上是去中心化、自行运作的。也就是说保险公司可以自行地运作和管理这些项目。这些项目上链后，通过引入这些参与方、监管机构、第三方媒体，甚至有些愿意参与的会员，他们可以对链上数据的真实性进行验证。



应用案例2：跨境汇款



图4-4 跨境汇款示意图

传统跨境汇款与银行间清结算过程中，痛点在于其流程需要经过开户行、央行、境外银行、代理行、清算行等多个机构，每个机构都有自己的账务系统，因此速度慢、效率低。腾讯云区块链TBaaS所拥有的共享账本和智能合约的特性，帮助用户解决银行间清结算慢，跨境汇款时间长，费用高以及银行单据繁多，处理流程时间长等问题。TBaaS所提供的完备智能合约集成开发调试环境，与其它平台不同，腾讯特别提供智能合约检查服务，对合规性和安全性进行校验，以防止类似于以太坊DAO安全事件的再次发生。



4.2 公证与记录

业务场景

- 1) 电子合同
- 2) 电子票据
- 3) 证据保全
- 4) 供应链金融/供应链管理

解决的业务痛点

- 1) 出证慢，流程长，票据作伪
- 2) 维权成本高

应用案例：供应链金融

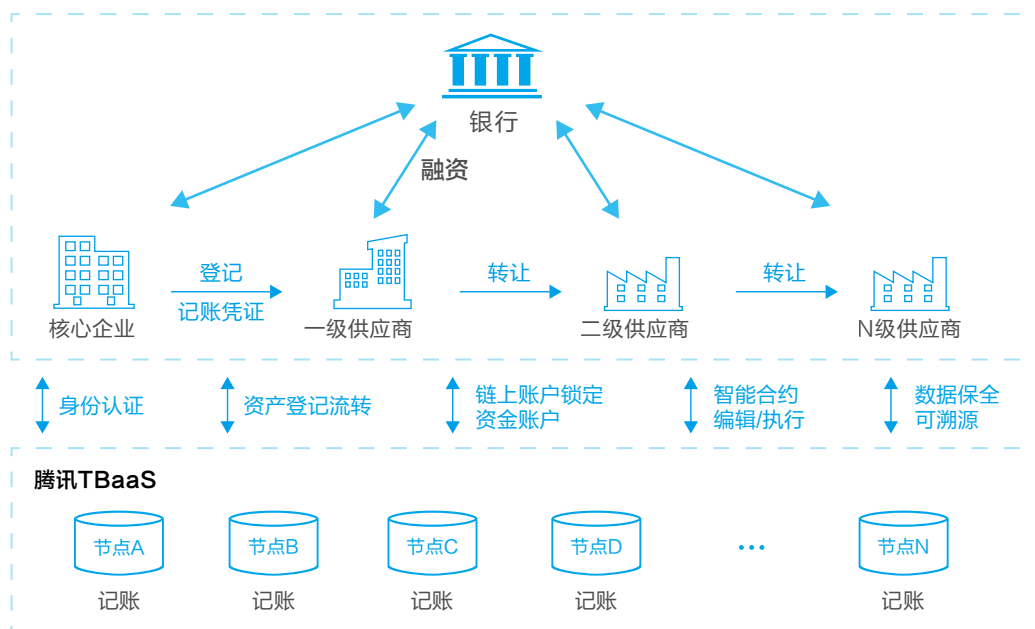


图4-5 供应链金融示意图



供应链金融简单来说就是银行围绕核心企业，管理上下游中小企业的资金流和物流，并把单个企业的不可控风险转变为供应链企业整体的可控风险。其核心目的就是为了降低资金成本，提高商业效率。传统的银行与企业金融服务中，基于风险管理的考虑，银行仅愿对核心企业有应收账款义务的上游供应商(一级供应商)提供保理业务(应收帐款融资)或是对其直接下游经销商(一级经销商)提供预付款融资或存货融资，银行利用核心企业的信用以及订单作为背书通常只贷款给核心企业和一级供应商，信任无法拆分成多级传递，处于供应链下游的供应商

面临融资难的问题。同时，各机构/企业间使用的非统一ERP系统，账务等数据无法共享，形成信息孤岛，对账清算异常繁琐。腾讯云区块链中共享账本技术解决供应链金融的核心问题，可以让供应链金融全流程所涉及的利益方都是共享账本的一个节点，所有在链上的参与方都可以读/写环节中交易的数据。共享账本所承载的供应链金融信息和价值可以自由分叉和合并地进行流转和价值传递。

腾讯云区块链TBaaS真正的能将交易数据，实现开放、一致、真实验证且不能篡改，银行能更好地管控风险和大幅降低银行作业成本。区块链技术发展与应用，将成为银行推广供应链金融业务最佳的解决方案，银行可以不再局限押品融资，而渐渐转向省时、不需控货和低操作成本的保理业务，服务更多的中小长尾用户群。

TBaaS 所具备的区块链防篡改特性可保障智能合约的执行，为智能合约提供运行的平台。在真实业务场景中，腾讯云区块链 TBaaS 可以有效地帮助客户解决了公证、信息记录与供应链链条中业务流程长，单据繁多和信息作伪与易篡改的问题。

4.3 互助保障

业务场景

- 1) 互助保险
- 2) 大病众筹
- 3) 公益捐赠

解决的业务痛点

- 1) 平台方作弊问题



2) 公益善款流向不透明

应用案例：互助保险

国内近两年兴起的互助保障，被广泛寄希望于借助互联网实现降低保费水平，惠及民众的目的。但作为新兴事务的互助保障，伴随着产业的快速兴起，也出现了各种各样的问题，同时由于规章制度，监管控制等政策法规尚未出台，互助市场也出现了很多不和谐的声音，目前互助保障可能出现的问题，主要集中在以下几点：

- 平台篡改投保人数
- 平台篡改投保时间、投保人身份
- 虚构患者，与鉴定机构、医院合谋欺诈
- 平台挪用保险资金
- 患者与医院合谋，虚夸病情，伪造用药或医疗服务
- 患者与鉴定机构合谋，超标准用药或医疗服务
- 鉴定机构与医院合谋

因为区块链具有无法篡改和追溯功能，利用互联网大数据来配合区块链这些技术，可能构建一个全网监管的体系，不仅能够提高监管的实时和效率，还能够降低监管的成本。在这些技术的推动下，社会会从制度监管走向技术监管，从公司的合规走向社会的监督体系。

我们将协助互助系统在现有平台基础上进行定制优化，在不影响现有系统正常运行的情况下，利用区块链技术实现信息保存，并实现区块链上的数据查询功能，将账目和清结算信息公开。

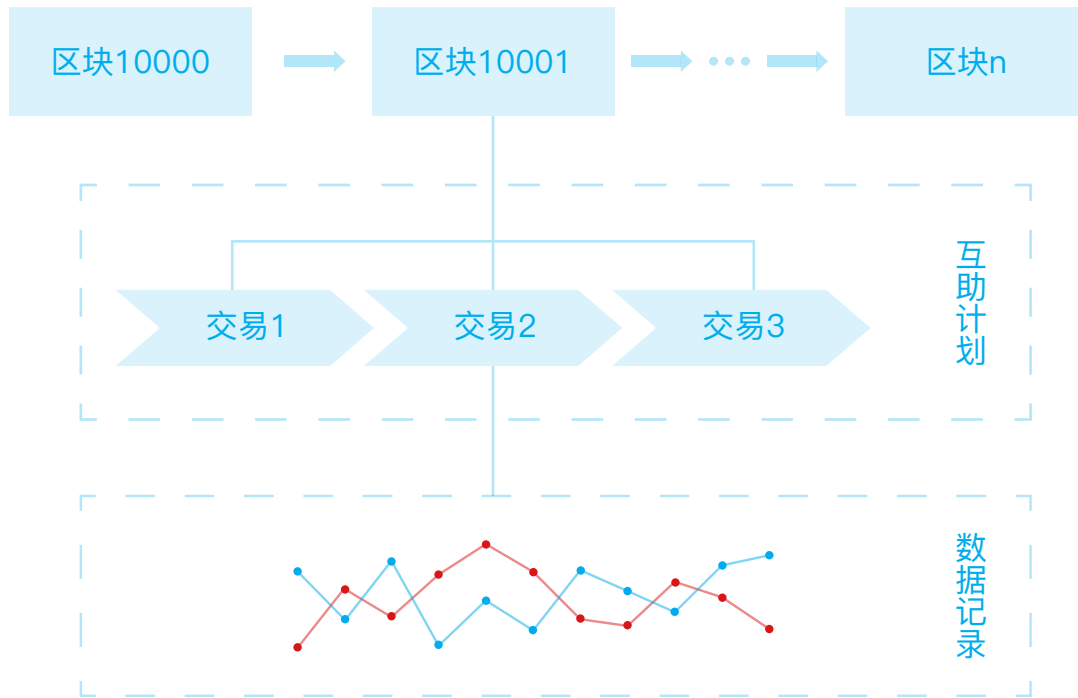


图4-6 互助计划数据上链

同时我们将协助互助保障系统使用区块链来构建底层平台。首先，用户所有资金划拨、资金全流程上链；其次，如果用户资金转为保险，比如为患者提供治疗资金。这本质上代表了这部分资金不仅上了链，而且在链上做了一笔资产的转换，即转换成了保险资产，那么这个保险资产有没有赔付、它的运行状况又如何，都可以在链上进行公示。所以，区块链同时成为了互助会员之间的爱心链和信任链。

我们利用区块链技术建立展示平台，将资金信息、互助项目信息、会员信息共享到区块链当中。其中除了涉及到存证能力之外，还有一项非常重要的方面就是治理能力。TBaaS平台可以引入监管机构、第三方媒体和会员，共同参与平台的监管。我们的平台是一个开放的平台，其业务模式上是去中心化、自行运作的。也就是说公益机构可以自行地运作和管理这些项目。这些项目上链后，通过引入这些参与方、监管机构、第三方媒体，甚至有些愿意参与的会员，他们可以对链上数据的真实性进行验证。



4.4 数字资产

业务场景

- 1) 大数据交易
- 2) 共享经济
- 3) 积分流通与通兑

解决的业务痛点

- 1) 共享经济
- 2) 数字资产交易
- 3) 积分流通与兑换

应用案例：预付费卡

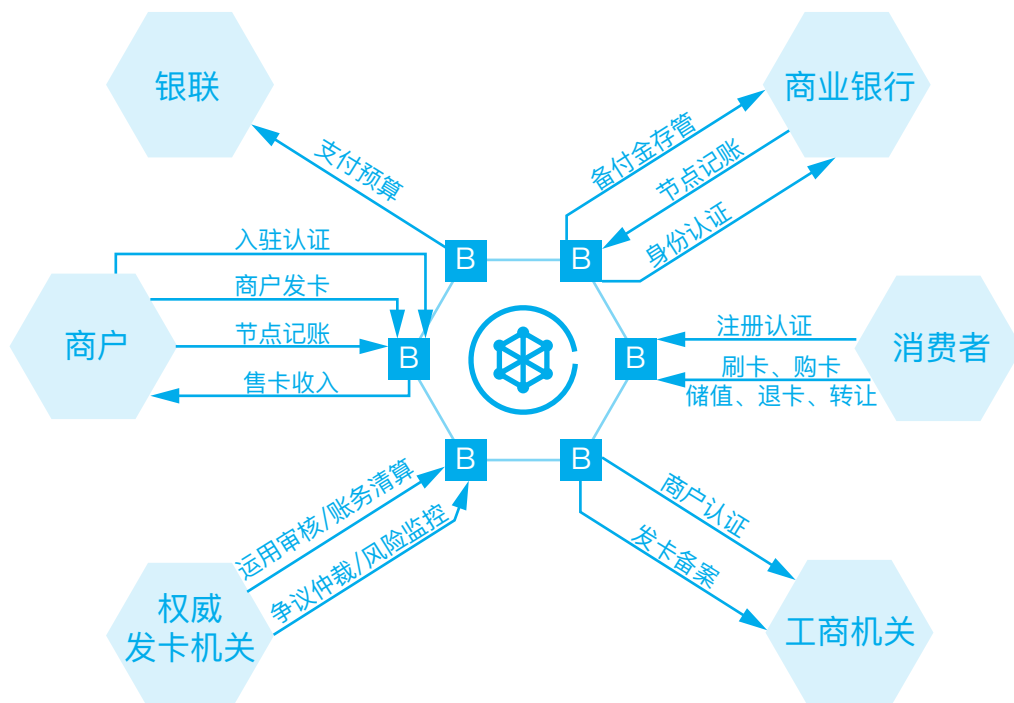


图4-7 预付费卡示意图



在银行预付费卡消费领域，2017年投诉量约5万件，年均增长约35.7%，其中不乏有发卡店铺关店走人，卷款跑路的问题；发卡方霸王条款，一经出售概不退换；以及服务缩水导致办卡前后态度截然不同，优惠难以兑现等问题。腾讯云区块链可以帮助银行将游离在监管视线外的单一用途预付费纳入监管范畴，提高宏观货币监管精确度，降低非法集资的可能性。同时，帮助商户可以保证预付费留在商户账户内的前提下，提高卡内资金通兑的效率，可以在一定程度扩大预付费使用的商户圈，增加了客源。区块链平台的征信体系帮助消费者甄别商户的信用，减少出现商户霸王条款的不良现象出现，提高商户跑路成本，通过合理的赔付机制降低客户损失风险。各项交易数据通过区块链技术可保证数据的不可篡改和可追溯，也帮助消费者在争议处理过程中，为争议解决也提供了有力的证据。

腾讯云区块链 TBaaS 提供价值流通能力，能够让区块链在数字资产发行与流通中扮演资产确权、交易确认、记账、对账和清算的角色；而区块链技术的防篡改能力，将有效防止数据篡改，规避内部作弊风险。

4.5 防伪溯源

业务场景

- 1) 医疗药品溯源
- 2) 烟草溯源
- 3) 食品溯源
- 4) 处方流转

解决的业务痛点

- 1) 商品伪造
- 2) 商品难溯源

应用案例1：农产品溯源

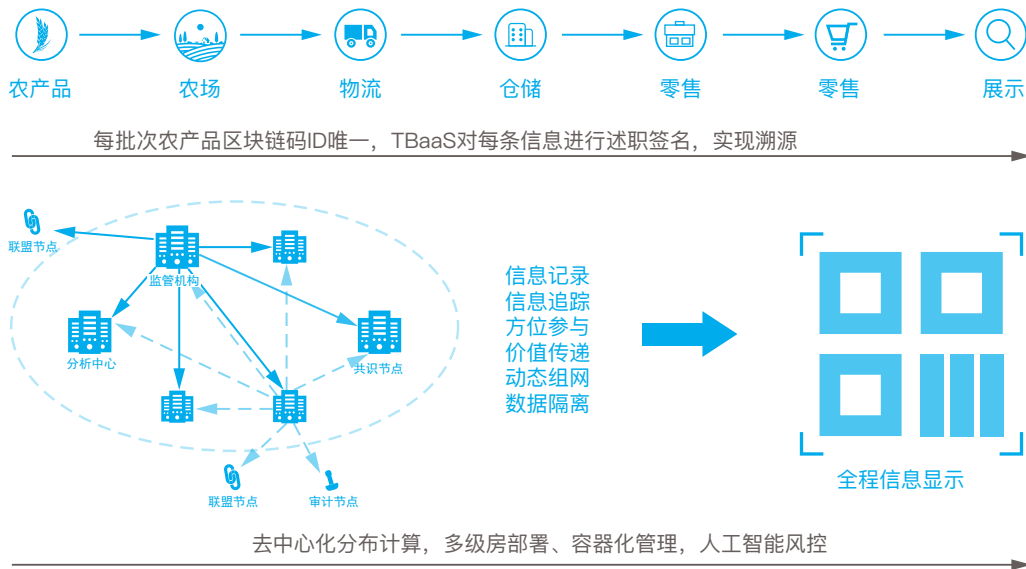


图4-8 农畜产品溯源示意图

某农场基于腾讯云区块链TBaaS平台提供的联盟链提供畜牧牲畜的溯源验证，让普通大众能够吃上放心肉，同时提高肉制品的品牌口碑和产品销量。TBaaS区块链系统对接农场线下养殖过程追溯平台数据库，记录牲畜养殖全过程。通过给牲畜佩戴RFID电子耳标作为标识载体赋予每个牲畜个体一个唯一标签标识码，将牲畜的基本信息，如牲畜出生记录、饲料使用记录、免疫记录、检疫记录和兽药使用记录等进行录入。牲畜屠宰环节在录入数据库屠宰地点，屠宰负责人，时间戳等。将记录了肉类信息的二维码防伪标签RFID粘贴在包装好的肉产品的包装表面上，同时保证做到一物一码，同时将此二维防伪标签RFID的标识数据生成唯一的数据指纹，并且采集到TBaaS区块链上。同时将此数据指纹录入工厂加工数据库供后续查验牲畜养殖，屠宰和加工等信息索引值。在物流环节，扫描包装上的二维码后，添加完善信息，添加仓库、运输车、肉制品包装图片等相关信息到物流系统数据库，同时针对这些信息重新生成数据指纹，图片的非结构化数据也生成数据指纹，同时保存在公共的云存储，供后面查询访问，新产生数据指纹同时录入TBaaS区块链。此方法在后续的仓储，零售环节重复使用，每个环节都会记录时间戳和相应的详细数据。TBaaS区块链记录牲畜经历整个供应链环节产生相应的数据指纹和包装上唯一的二维码。最终用户在购买肉制品时，可以根据此二维码在最后的消费环节展示整个肉制品历史数据的追溯。



应用案例2：微信智慧医院处方安全流转平台

腾讯微信智慧医院某省人民医院的项目中，基于TBaaS平台提供的联盟链，确保医生给患者开具的处方（电子版），在医院药房或者社会药房取药时，患者的隐私信息保密，处方开具方身份合规，处方内容无篡改；

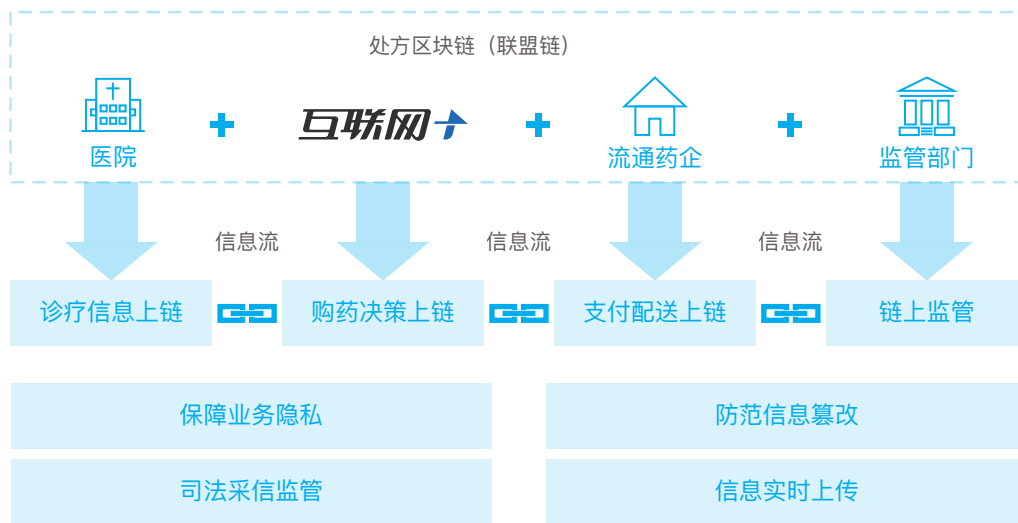


图4-9 处方流转示意图

在这个联盟链中，腾讯微信智慧医院与各参与方一起构建联盟，卫计委、医院、药企、患者上链，每个流通环节和状态更新都产生链上hash值。因为区块链的防篡改特性，一旦发生纠纷，监管部门随时可查询溯源。



4.6 物联网

业务场景

- 1) 智能家居
- 2) 物流供应链
- 3) 智能制造

解决的业务痛点

- 1) 物联网中心化架构成本高昂
- 2) 信息易篡改，隐私保护弱
- 3) 制造企业难以根据市场情况动态调节采购和生产

应用案例：智能制造

区块链技术的出现，其点对点的组网模式、分布式的存储、安全的数字认证方式，天然的与物联网的诉求相契合，不仅填补了物联网在实际应用中的缺陷，也使物联网真正大规模部署、安全运营成为可能。针对行业上的痛点，腾讯TBaaS平台，助力物联网与区块链技术的结合，不仅降低了物联网的运营成本，还使得智能设备能够以更加安全可靠的方式进行管理，并实现物联网的高级目标，即支付与费用的结算，形成价值流通的网络。

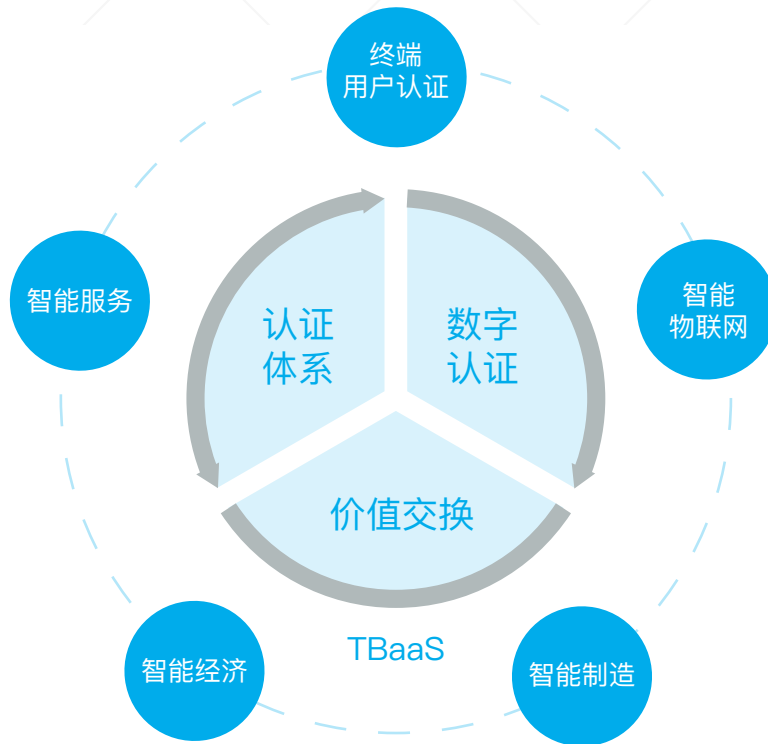


图4-9 区块链助力物联网实现价值流通

物联网在企业中的应用，结合区块链平台，对原有的商业模式的创新，形成了物联网+的转变。企业借助物联网+区块链，实现了信息的快速互联互通，实现了价值的无障碍交换，真正意义上将变革技术引入业务流程中，在此基础上再结合大数据、AI、云计算等，进而实现传统制造企业向数字服务企业的转变。

随着时代的变化，传统的重资产制造企业，面临着诸多困境，成本上升，盈利水平下降，创新能力不足，正困扰着企业向现代化更有竞争力的公司转变。针对这一难题，腾讯云TBaaS平台为企业提供全方位的服务，结合云上的AI、大数据，云计算等，协助企业对自身进行改造。

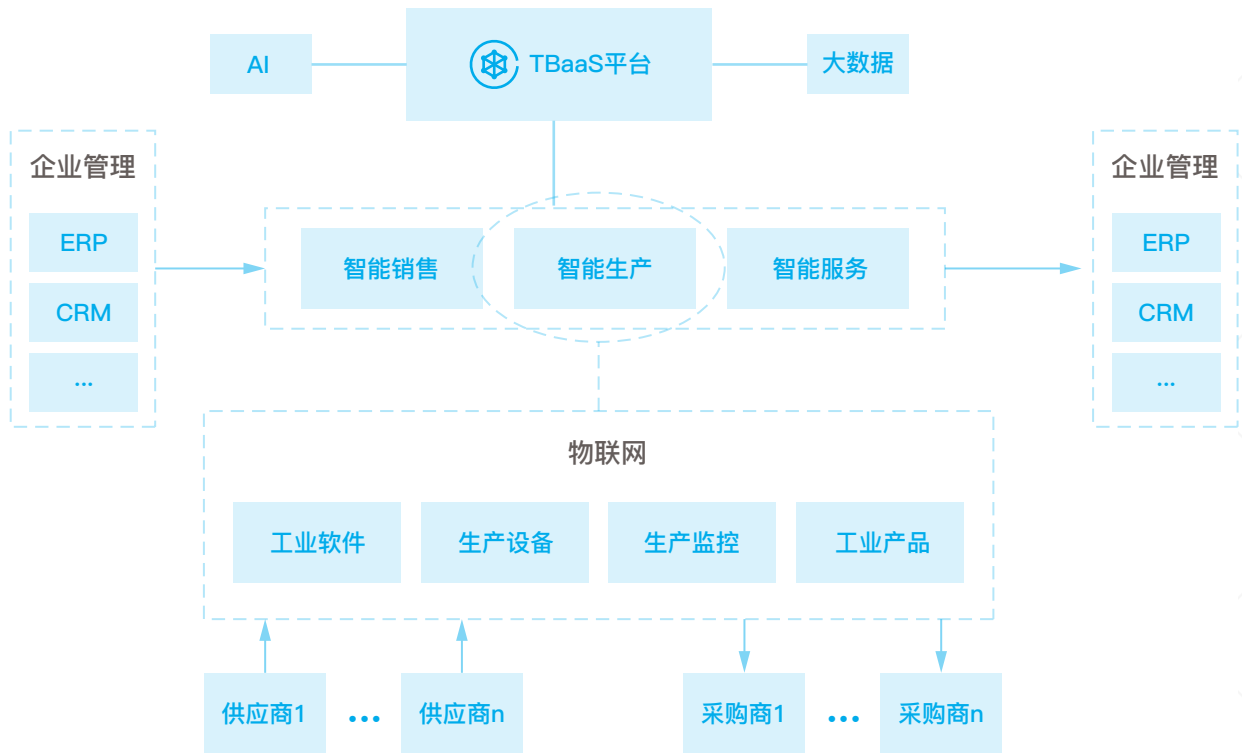


图4-10 TBaaS参与智能制造过程

通过引入区块链平台，将企业采购、生产、销售的上下游联通。核心企业的生产原材料或零部件，需要来自众多供应商，通过TBaaS平台，实现各供应商的生产和供货时间上的统一协调，同时能够对零件供应进行溯源和跟踪，减少供货时间，并更可靠追踪供货质量；核心企业的生产，可以采购商可以将采购订单进行按需生产，根据市场情况动态调节，最大限度的减少库存和盲目生产；在企业内部的生产流程中，区块链平台的引入，实现了企业的智能制造，借助物联网产生的数据，企业不仅能够随时按照上下游的信息进行动态调节生产，还能将生产的数据实时上链，为智能销售，智能服务提供依据。



通过物联网的信息上链，核心企业可以感知用户产品的状态，是否需要更换零部件或新的设备，提前通知客户并实现自主生产，减少客户的备货等待时间。更重要的是将制造企业向服务企业转变提供保障，核心企业可依据TBaaS平台并结合的腾讯云上的AI、大数据分析等引擎，确立对市场的动态感知，用户行为的分析，为市场、为用户提供咨询服务、商品服务和决策服务，实现制造即服务的转变。

4.7 共享经济

业务场景

- 1) 电力共享
- 2) 充电桩共享
- 3) 房屋共享

解决的业务痛点

- 1) 资源闲置浪费
- 2) 缺乏交易协商机制

应用案例：智能电网

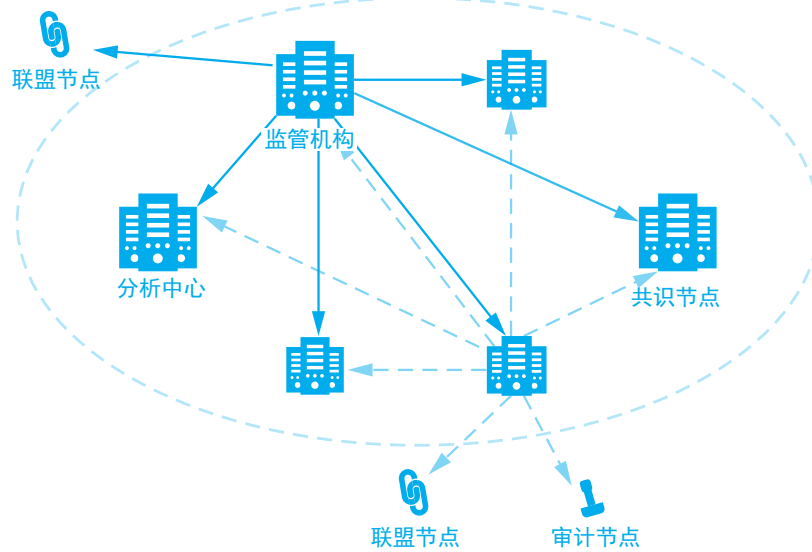
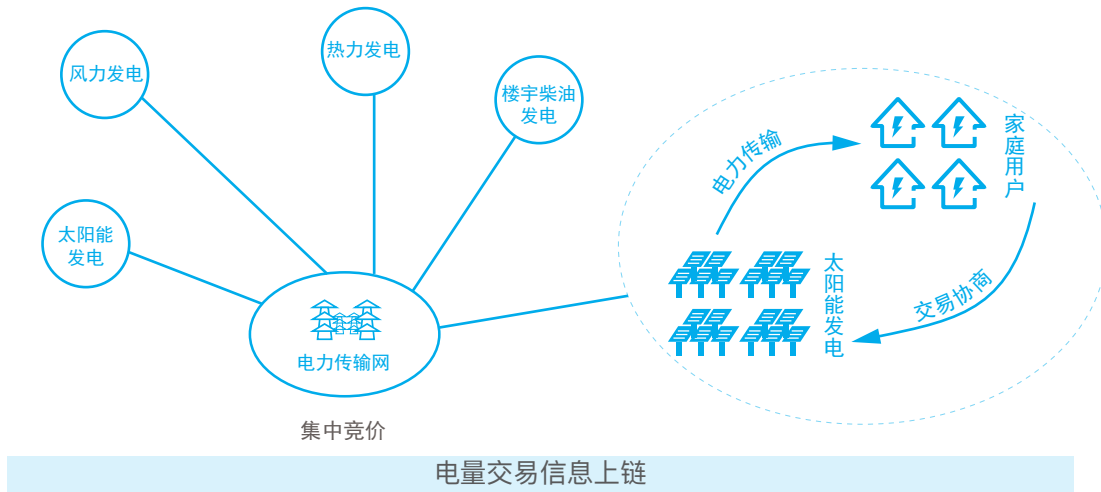


图4-11 电力共享实现价值交换

某小区，地处沿海平原城市，日照资源丰富，是太阳能电力的理想来源地，但是当地天气变化波动大，较难预测。天气晴朗的时节，产生的电源远远超过家庭使用量，由于家庭缺乏有效的电力储存设备，造成清洁电力能源白白浪费；另一方面，缘与历史原因，能源电力市场一直是基于地区性公用事业垄断者的模型和远程输电基础设施所主宰。由于太阳能清洁能源缺乏稳定可预测的生产量，加之总体容量达不到最低电力交易阈值，一直无法纳入当地集中式电力交易市场。消费者开始寻求一个有效的分布式的交易平台和去中心化能源交易的协商机制，通过自产能源或基于储存解决方案的能源套利来直接参与能源购买决策。最终创造一个更加去中心化，低交易成本的电网交易平台。腾讯TBaaS区块链平台提供这个电网交易平台的共享账本。在整个社区搭建智能电网基础设施



施，借助安装在居民家里的智能电表双向多种费率计量功能、多种数据传输模式的双向数据通信功能，电力消费者可以根据他们的能源需求进行自动响应。每一个固定时间周期，共享电力市场协商公布一个价格，电力生产者和消费者的代理机器可以直接查询这个协商价格，由于分布式电力资源不需要输配电设施投资，通常价格相对市电有更具吸引力的折扣，促成电力更容易达成销售交易。当达成电力交易后，交易登记到腾讯TBaaS区块链账本，同时线下通知输电调度员将电网的电力从供给节点传输电力到需求消费节点。

未来将引入更丰富的电力来源，譬如风力发电，智能楼宇储备的富余柴发机电力和传统的热力、水利发电等，最终构建更经济环保的去中心化的共享电力市场，让消费者最终拥有更多选择权。



5. 未来展望

腾讯云一直坚持建立开放生态，希望与合作伙伴共同打造区块链的生态环境。腾讯云积极的参与制定区块链行业标准，与业界领先的厂商进行合作，拓展腾讯云区块链即服务对各类区块链底层平台的支持，从而更好的适配不同的用户场景；加强和各监管机构的合作，公开内部的控制情况，打造合规、透明的服务平台。同时，腾讯云积极引入周边生态伙伴，一起提供各个行业的区块链通用解决方案和定制化解决方案，为客户的区块链业务快速开展提供坚实的基础。未来，我们着重推动腾讯云区块链在以下几个方面的发展：

5.1 多种平台支持——让客户更专注于自身业务

由于目前区块链技术尚处在高速发展的时期，目前已经出现了很多区块链基础技术。因此，在具体选择使用哪种技术方案时，我们坚持以用户和应用为导向，根据用户实际应用场景的性能、功能要求，以及未来可预见的扩展需要为出发点，选择具体的底层技术平台，配置系统参数，让区块链技术与应用完美配合，发挥出应有的作用。

在很多要求使用区块链的场景中，合规性和安全性是企业用户所无法避免的话题。区块链的合规性和安全性除了体现在可监控、可管理等系统功能要求方面外，还需要符合行业规范、满足可信准入机制等特殊规定。我们通过对各类区块链底层平台的支持，使其能够满足各类客户、各种应用场景的需求。

腾讯云区块链即服务平台在未来将提供多种区块链解决方案，除了目前已经支持Linux基金会的超级账本(Hyperledger Fabric)、还将支持R3 Corda、企业以太坊(EEA)等多种技术，TBaaS平台将为这些异构区块链平台进行了封装，屏蔽其底层的差异，上层为用户提供相同的能力。企业或金融机构将更关注在如何把区块链技术应用到业务中，提升业务效率或服务质量，而不需要聚焦底层区块链技术的开发和设计，极大的解决了应用落地周期长的难题。



图5-1 腾讯云区块链平台

5.2 链外信任——通往现实世界的桥梁

链外信任是阻碍智能合约通往现实世界的一大难题，目前智能合约的执行所依赖的输入基本局限于链内，如何能够将智能合约执行所依赖的条件拓展为跨链以及链外是当前很多业界同行重点发力的方向。腾讯云区块链作为一个开放平台，将积极拥抱业界其他优秀区块链系统，致力于成为区块链世界的跨链信息枢纽，帮助客户充分利用平台枢纽优势，降低客户跨链成本并快速实现互信。

5.3 引领未来——用开放的心态拥抱未来

在过去20余年里，互联网为我们带来商业模式的变革，极大提高了组织和个人的效率，让信息实现了高效流动。然而交易的基本机制始终没有改变，区块链带来的透明和效率，或将颠覆交易本质。

区块链系统的去中心化使整个网络内的自证明功能成为现实，人们可以低成本地实现信息“价值”的传递。我们相信，随着社会进步，区块链技术的应用将带来新的商业规则和文明形态，扁平化大小机构的商业信息能力和成本差距，帮助企业重塑形态，改进社会结构。

站在科技浪潮之巅，腾讯云区块链将怀抱开放的心态，充分利用云端优势积极探索和创新，引入并连接周边生态合作伙伴，帮助客户降低上链门槛，扩大企业边界，高效地完成企业间协作，最终实现价值的自由流动。



6. 参考文献

1. S. Nakamoto, Bitcoin: A peer-to-peer electronic cash system (2009): <https://www.bitcoin.org/bitcoin.pdf>
2. Blockchain Technology Beyond Bitcoin, UC Berkeley. (2015)
3. Is Blockchain the Next Big Disruption? , Neeley School of Business TCU. (April 2017)
4. Gmane.Org (2008): <http://article.gmane.org/gmane.comp.encryption.general/12588/>
5. 工信部：中国区块链技术应用和发展白皮书(2016)
6. 麦肯锡：区块链-银行业游戏规则的颠覆者(2016)
7. Don T, Alex T. (October 2016): Blockchain Revolution
8. 高盛：区块链从理论走向实践(2016)
9. Bashir, Imran (2017). Mastering Blockchain. Packt Publishing, Ltd. ISBN 978-1-78712-544-5.
10. BlockchainHub. (January 19, 2018): "Blockchains & Distributed Ledger Technologies".
11. Hyperledger Fabric Website: <https://www.hyperledger.org/projects/fabric>
12. Hyperledger Blockchain Project Is Not About Bitcoin". Retrieved October 17, 2016
13. Mazonka, Oleg. (December 29, 2016): Blockchain: Simple Explanation. Journal of Reference.
14. A Next-Generation Smart Contract and Decentralized Application Platform, <https://github.com/ethereum/wiki/wiki/White-Paper#bitcoin-as-a-state-transition-system>
15. UK Government Chief Scientific Adviser (2016) : Distributed Ledger Technology: beyond block chain
16. Brown, R. G. (2016). Introducing R3 Corda: A Distributed Ledger for Financial Services.



腾讯云