腾讯区块链方案白皮书

打造数字经济时代信任基石

发布：腾讯FiT（支付基础平台与金融应用线）、腾讯研究院

编制：腾讯FiT、腾讯研究院、腾讯公共战略委员会办公室、腾讯CDG战略发展部

时间：2017年4月

最新、最in的重磅行业分析、研究报告，每日微信群内免费分享!

扫一扫二维码，关注微信公众号，

点击菜单“专业社群”，加入“IT大佬”微信群，获取免费报告!

[报告仅用于分享学习使用，不做任何商业用途！]

前言

区块链技术给数字经济时代带来了巨变的曙光。

这种巨变在互联网近 50 年的历史上曾发生过两次。第一次巨变是全球性的联网，自 1969 年阿帕网诞生以来，全世界主流国家逐渐接入互联网，开启了全球联网的征程。第二次巨变是全球性的应用，自 1989 年万维网论文问世后，互联网应用全面开花，实现了应用全球爆发。

第三次巨变正在酝酿。2009 年比特币诞生是个标志性事件。在区块链技术的支持下，比特币打破了传统纸币的“暗黑”盒子。作为实体的纸币的流通是看不见的，没有人知道一张纸币从哪里来到哪里去，而区块链却可以让数字货币的每一笔动向都清清楚楚有“链”可查，同时还可以保护参与者的隐私。

人们发现，区块链的意义在于可以构建一个更加可靠的互联网系统，从根本上解决价值交换与转移中存在的欺诈和寻租现象。越来越多的人相信，随着区块链技术的普及，数字经济将会更加真实可信，经济社会由此变得更加公正和透明。

进一步的研究发现，区块链技术具备一种“降低成本”的强大能力，能简化流程，降低一些不必要的交易成本及制度性成本。这种能力应用于许多社会领域中，对于改善当前低迷的经济环境更有现实意义。

区块链引发了世界性的关注，迅速地成为一场全球参与竞逐的“军备”大赛，许多国家认识到区块链技术巨大的应用前景，开始从国家层面设计区块链的发展道路。

2017 年，区块链及相关行业加速发展，全球正在跑步进入“区块链经济时代”。在全球范围内，会出现更多的成熟应用。此时此刻，中国面临重大机遇。

编委会成员

顾问：卢山、郭凯天、赖智明、江阳、Brentirvin、许国爱

策划与协调：郭锐、司晓、刘勇、唐羚

研究撰写：张孝荣、杨思磊、史琳、巴洁如、徐思彦、郭承肯、顾文洁
梁军、李茂材、王宗友、朱大卫、张建俊、屠海涛、赵琦、李政、秦青

目录

第1章. 区块链的兴起和未来之路

区块链的诞生，标志着人类开始构建真正可以信任的互联网。通过梳理区块链的兴起和发展可以发现，区块链引人关注之处在于，能够在网络中建立点对点之间可靠的信任，使得价值传递过程去除了中介的干扰，既公开信息又保护隐私，既共同决策又保护个体权益，这种机制提高了价值交互的效率并降低了成本。

从经济学意义来看，区块链创造的这种新的价值交互范式基于“弱中心化”，但这并非意味着传统社会里各种“中心”的完全消失，未来区块链将出现大量的“多中心”体系，以联盟链、私有链或混合链为主，区块链将会进一步提高“中心”的运行效率，并降低其相当一部分成本。

从技术角度来说，我们认为，区块链是一种由多方共同维护，以块链结构存储数据，使用密码学保证传输和访问安全，能够实现数据一致存储、无法篡改、无法抵赖的技术体系。这种技术给世界带来了无限的遐想空间，全球对区块链的关注热度持续升温，全球主要经济体从国家战略层面开始对区块链技术及发展趋势进行研究。

1.1. 区块链的兴起

1.1.1 从摆脱第三方制约起步

早先，人们将区块链视为点对点网络上的一个分类账本，每笔交易自诞生起，所有转账、交易都将被记录在“区块”上，区块与区块之间首尾相连，形成链式的结构，并且公布给该网络上所有的节点，节点之间通过共识机制形成共识。节点成员可根据权限查阅相关交易记录，但任何单个节点都无法轻易控制和更改整个网络的数据。

这种设计来源于 2008 年中本聪发表的论文《比特币：一种点对点的电子现金系统》。文章提出，希望可以创建一套新型的电子支付系统，这套系统“基于密码学原理而不是基于信用，使得任何达成一致的双方能够直接进行支付，从而不需要第三方中介参与”。

该论文催生了比特币，标志着人类社会的货币体系向前迈出了一大步。比特币采用了公开的分布式账本的设计思路，真正摆脱了第三方机构的制约。随后比特币进入快速发展期。

2009 年 1 月 3 日，区块链的第一个区块诞生，该区块又名“创世区块”。

2009 年 1 月 12 日，中本聪发送了 10 个比特币给密码学专家哈尔芬尼。

2010 年 7 月，比特币交易所 Mt.Gox 的成立，比特币的价值被世界认可。

此后几年里，由于比特币的挖矿机制造成巨大的资源消耗，比特币的匿名性对传统金融监管提出了挑战，使得比特币价格随之出现了大起大落。

1.1.2 从比特币跃迁到区块链+

区块链的诞生，标志着人类开始构建真正的信任互联网。

有一种新的观点认为，区块链技术可以构建一个高效可靠的价值传输系统，推动互联网成为构建社会信任的网络基础设施，实现价值的有效传递，并将此称为价值互联网。我们注意到，区块链提供了一种新型的社会信任机制，为数字经济的发展奠定了新基石，“区块链+”应用创新，昭示着产业创新和公共服务的新方向。

区块链技术已经在全球开始部署应用，美、英、日、德、加、澳等发达国家已经认识到区块链技术在公共服务和社会机制优化上存在着巨大的应用前景，开始设计区块链的发展道路。目前主要有两大应用趋势：

从公共服务层面来看，区块链技术正在探索在公共管理、社会保障、知识产权管理和保护、土地所有权管理等领域的应用。相关实践表明，这种技术有助于提升公众参与度，降低社会运营成本，提高社会管理的质量和效率，对社会管理和治理水平的提升具有重要的促进作用。

从经济社会来看，区块链经济已经萌芽。许多基于区块链的解决方案，可以改善现有的商业规则，构建新型的产业协作模式，提高协作流通的效率。无论是各国央行和各大商业银行，还是联合国、国际货币基金组织以及许多国家政府研究机构，都对“区块链+”投入极大关注。

区块链可为经济社会转型升级提供系统化的支撑。区块链+的显著优势在于优化业务流程、降低运营成本、提升协同效率，这个优势已经在金融服务、供应链管理、知识产权、智能制造、社会公益以及教育就业等社会各领域初步体现出来。

1.2. 区块链的设计思想

价值交互的基础是双方信任的建立。区块链技术的革命性在于它实现了一种全新的信任方式，通过在技术层面的设计创新，使得价值交互过程中人与人的信任关系能够转换为人与技术的信任，甚至于由程序自动化执行某些环节，商业活动得以更低成本的实现。

1.2.1. 经济层面的设计思想

降低成本，是区块链技术的一个重要的设计思想。在区块链体系中，参与者可以不需要了解对方基本信息的情况进行交易，实现了“无需信任的信任”，改变了传统模式中以第三方为中心的信任模式。

这种设计模式有许多创新性，其中两项值得关注：

第一，交易信任由机器和算法确定。区块链通过构建一个依赖于机器和算法信任的交易体系，解决在匿名交易过程中的相互信任问题。所有参与者将在无须建立信任关系的环境中，通过密码学原理确定身份，依靠共识机制实现相互间的信任。

第二，交易过程可以由程序自动执行。区块链通过可编程的智能合约，自动执行双方所达成的契约，排除了人为的干扰因素，从制度上防止任何一方的抵赖。从而推动经济社会进入一种智能的状态，实现当前经济交易系统的质的飞跃。

基于区块链技术的“弱中心化”特性，现有的经济体系可以脱离当前通过制度约束或第三方机构背书，双方直接实现价值交付。这种“弱中心化”特性可以有效降低交易成本，提高交易效率，减少因交易一致性所引发的摩擦。

1.2.2. 技术层面的设计思想

通俗的说，区块链可以看成是一套由多方参与的、可靠的分布式数据存储系统，其独特之处在于：一是记录行为的多方参与，即各方可参与记录；二是数据存储的多方参与、共同维护，即各方均参与数据的存储和维护；三是通过链式存储数据与合约，并且只能读取和写入，不可篡改。

在应用实践中，这种系统能够实现所有参与者信息共享、共识、共担，可以成为各种商业行为和组织机构的基础技术架构。具体与传统中心式系统对比如下表所示：

系统分类 / 关键点		传统技术系统		区块链技术系统	
		特点	中心化的实现方式	特点	去中心化的实现方式
记录行为的多方参与	网络架构	中心化	主从式的B/S网络	去中心化	P2P分布式网络
	记录权及记录方式	中心节点进行	中心节点记录及维护所有交互数据	所有节点参与	共识算法确定记录权，共同维护交互数据
	交易方式	每笔交易需中心节点确认	中心节点监督和维护	点对点交易	所有节点集体监督和见证
	信任关系	中心节点见证	中心节点为所有节点进行信任背书	节点自证其信	非对称加密技术验证身份，零知识证明等方式验证信息
	交易一致性	中心节点保障交易数据的一致性	中心节点的一本账，保障交易数据的一致性	所有节点共同参与解决数据交易的一致性	所有节点通过共识算法保证交易一致性，解决双花现象
账数据存储的多方维护	交易有无欺诈	存在欺诈和造假的可能	中心节点主动欺诈的可能	不可欺诈、不可造假	分布式存储、共识算法
	信息被篡改	存在数据被篡改和抵赖的可能性	中心节点存在被攻击、数据被篡改等可能性	不可篡改、不可抵赖	分布式存储、链式数据结构、哈希算法、时间戳及数字签名
	数据存储的可靠性	中	依靠中心节点进行交易信息系统的存储和容灾备份	高	任意单个节点故障或者少数节点故障，系统能正常运行，并且故障节点数据可以恢复。
	隐私保护	交易双方身份信息存在泄露的可能性	所有参与交易者需提供身份信息，且都由中心节点保存，中心节点存在被攻击、盗取等可能，导致交易者的隐私泄露	交易双方的身份信息不会被泄露	所有参与方在区块链中通过加密后的ID进行标识。 1、不需要所有交易者提供身份隐私信息，保障交易者的隐私不被泄露。 2、同一个交易者可通过多个ID进行的多次交易来达到隐私保护的目的。

1.3. 区块链的核心技术

区块链技术不是一个单项的技术,而是一个集成了多方面研究成果基础之上的综合性技术系统。我们认为，其中有三项必不可缺的核心技术，分别是：共识机制、密码学原理和分布式数据存储。

第一，共识机制

所谓共识，是指多方参与的节点在预设规则下，通过多个节点交互对某些数据、行为或流程达成一致的过程。共识机制是指定义共识过程的算法、协议和规则。

区块链的共识机制具备“少数服从多数”以及“人人平等”的特点，其中“少数服从多数”并不完全指节点个数，也可以是计算能力、股权数或者其他的计算机可以比较的特征量。“人人平等”是当节点满足条件时，所有节点都有权优先提出共识结果、直接被其他节点认同后并最后有可能成为最终共识结果。

第二、密码学原理

在区块链中，信息的传播按照公钥、私钥这种非对称数字加密技术实现交易双方的互相信任。在具体实现过程中，通过公、私密钥对中的一个密钥对信息加密后，只有用另一个密钥才能解开的过程。并且将其中一个秘钥公开后（即为公开的公钥），根据公开的公钥无法测算出另一个不公开的密钥（即为私钥）。

第三、分布式存储

区块链中的分布式存储是参与的节点各自都有独立的、完整的数据存储。

跟传统的分布式存储有所不同，区块链的分布式存储的独特性主要体现在两个方面：一是区块链每个节点都按照块链式结构存储完整的数据,传统分布式存储一般是将数据按照一定的规则分成多份进行存储。二是区块链每个节点存储都是独立的、地位等同的，依靠共识机制保

证存储的一致性，而传统分布式存储一般是通过中心节点往其他备份节点同步数据。数据节点可以是不同的物理机器，也可以是云端不同的实例。

1.4. 未来发展趋势

区块链将对现有的经济社会产生巨大的影响，有望重塑人类互联网活动形态。

对于区块链近期的发展趋势主要有以下几个方面：

第一、应用模式升级。鉴于公有链的安全性及交易量与日俱增对现网容量之间的平衡问题，未来区块链的应用领域将以联盟链、私有链或混合链为主。比特币模式增加了区块链网络的维护成本，对于低价值、低风险的交易来说并非完全适用。考虑到效率及安全的提升，未来将是以联盟链、私有链、或由联盟链和私有链组成的混合链组成。

第二，多中心化。未来区块链系统架构将是构建可信任的多中心体系，将分散独立的各自单中心，提升为多方参与的统一多中心，从而提高信任传递效率，降低交易成本。即在信息不对称、不确定的环境下，建立满足各种活动赖以发生、发展的“信任”生态体系。

第三，从金融创新带动其他行业应用突破。区块链的应用领域将先从对交易各方有相互建立信任的需求，但又不容易建立信任关系的领域切入，如金融、证券、保险等领域。随着应用普及和社会认知度的提高，区块链将逐渐向社会各领域渗透。比如区块链已经初步的应用于政治选举、企业股东投票、博彩、预测市场等领域。

第四，智能合约的社会化。未来，所有的契约型的约定都实现智能化，利用智能合约可以保障所有约定的可靠执行，避免篡改、抵赖和违约。除了将社会中的有形资产转变为数字智能资产进行确权、授权和实时监控外，区块链还可应用于社会中的无形资产管理，如知识产权保护、域名管理、积分管理等领域。

第2章. 全球跑步进入区块链经济时代

区块链带来了效率提升和成本降低的技术手段，为经济社会发展和治理提供新的思路。围绕区块链体系，能够创造出丰富的产品和服务，人们可以在相互无信任的情况下，无地域限制地进行大规模协作。由此，一个全新的经济时代展现在公众面前。

区块链经济的前景极为壮阔，一种乐观的预测认为，到 2025 年之前，全球 GDP 总量的 10%将利用区块链技术储存。

现在，区块链经济已经处于爆发前夜。金融行业的探索领先一筹，而其他行业的应用正在快速展开。区块链行业应用具有明显的效益的显著优势在于优化业务流程、降低运营成本、提升协同效率，这个优势已经在金融服务、物联网、公共服务、社会公益和供应链管理等社会领域逐步体现出来。

2.1. 正在萌芽的区块链经济

区块链经济的发展，可分为三个阶段：

第一阶段是酝酿期，时期为 2009-2012 年，经济形态以比特币及其产业生态为主。

第二阶段是萌芽期，时期为 2012-2015 年，区块链随着比特币进入公众视野，新生的钱包支付和汇款公司出现，区块链经济扩散到金融领域。区块链底层技术创新不断。区块链技术从比特币系统中剥离出来。

第三阶段是发展期，2016 年开始探索行业应用，出现了大量区块链创业公司。预计 2017 年将进入到行业应用的爆发期。区块链经济的前景极为壮阔。未来基于现有互联网络、移动通

信等基础设施，区块链将进一步实现社会资金、合约、数字化资产在互联网上的交换、交易与转移，构建一个全新的依赖于机器和算法的诚信价值交换体系。

我们认为，区块链技术优先适用的经济领域至少具备以下三个特征：标准化程度高、自动化需求大、资质证明要求多。区块链技术应用将率先在具备这些特性的应用领域中凸显经济价值和优势。

2.2. 整体经济规模及趋势

当前，区块链经济处于爆发期前夜。金融行业应用已经相对广泛，其他行业的应用情况也进入了探索研发阶段。就这种新型经济形态未来体量，有测算如下：

据达沃斯论坛创始人克劳斯·施瓦布（Klaus Schwab）认为，区块链作为继蒸汽机、电气化、计算机之后的第四次工业革命的重要成果，预计到 2025 年之前，全球 GDP 总量的 10%将利用区块链技术储存。

根据市场研究机构 Gartner 预测，2020 年，基于区块链的业务将达到 1000 亿美元，除金融业外，制造业和供应链管理行业将为区块链带来万亿美元级别的潜在市场。

研究咨询公司 MarketsandMarkets 在专题调研报告[1]中预测，2016 年至 2021 年之间，全球区块链市场应用和方案供应商的复合年均增长值将达到最高。这类供应商的业务包括支付、文件证明、交易和其它用于提高企业运作效率的方案。

在区块链技术所涉及的行业中，银行、证券业和保险业所占市场份额最高。未来，区块链技术主导下的娱乐和媒体行业发展速度将持续加快，医疗健康、物联网、供应链等行业应用则紧随其后。

[1]Blockchain Technology Market by Provider, Application, Organization Size, Vertical, and Region - Global Forecast to 2021, MarketsandMarkets

从地区市场角度分析，2016 年北美区块链市场所占份额最高。2016 年到 2021 年期间，亚太地区的复合年均增长率将实现最大化 ,澳大利亚和中国将优先从区块链技术的诸多潜力中获益。

2.3. 区块链经济的全球化轨迹

区块链的应用价值得到全球广泛关注。发达国家认识到区块链技术巨大的应用前景，开始从国家层面思考区块链的发展道路。中国与世界同步，也启动了相关的研究和实践。

2.3.1. 美国

2015 年 1 月 26 日，纽交所入股的 Coinbase，获批成立比特币交易所，美国以纽约州为代表的比特币监管立法进程初步完成。

2015 年 6 月，纽约金融服务部门发布了最终版本的数字货币公司监管框架 BitLicense，美国司法部、美国证券交易所、美国商品期货交易委员会、美国国土安全部等多个监管机构从各自的监管领域表明了对区块链技术发展的支持态度。

2016 年 6 月，美国国土安全部对 6 家致力于政府区块链应用开发的公司发放补贴，以便让企业研究政府的数据分析、连接设备和区块链。国防部正致力于研发一个去中心化的分类账，以保证地面部队通讯及后勤免受外国侵扰。

除了政府外，产业界也开始纷纷在区块链技术展开布局。2015 年年底，各大金融机构都加大了区块链技术研究力度。硅谷的科技巨头纷纷推出了区块链项目。

2.3.2. 欧盟

2016 年 2 月，欧盟委员会把加密数字货币放在快速发展目标领域的首位，这项举措推动了各个机构针对数字货币的政策研究。

同年 4 月 18-21 日，欧洲数字货币与区块链技术论坛(EDCAB)为欧盟议会的政策制定者举办了一个集中讨论区块链的“博览会”。同时，欧洲中央银行表示，欧洲央行计划对区块链和分类账簿技术与支付、证券托管以及抵押等银行业务的相关性进行评估。

2.3.3. 加拿大

承认比特币的“货币地位”。2013 年 12 月，世界上首个比特币 ATM 机在温哥华投入使用，并修订法案规范比特币业务。2016 年 6 月，加拿大央行展示了利用区块链技术开发的 CAD-Coin——电子版加元。

2.3.4. 英国

英国政府 2016 年 1 月发布关于区块链的研究报告《区块链：分布式账本技术》，第一次从国家层面对区块链技术的未来发展应用进行了全面分析并给出了研究建议。白皮书建议将区块链列入英国国家战略，并推广应用于金融、能源等领域。6 月，英国政府进行了区块链试点，跟踪福利基金的分配以及使用情况。据英国工作与养老金部称，政府希望这一计划能够提供金融参与度的深度信息，并为财政预算提供支持。

2.3.5. 俄罗斯

俄罗斯互联网发展研究所（Internet Development Institute）准备了一个名为“经济与金融”的路线图，包括管理区块链的提议。在 2017 年 1 月，关于“合法化”区块链技术的发展路线图提交给了普京总统，对技术发展的未来法律框架进行了规划。

莫斯科市政府实行“积极公民”计划，希望通过区块链技术记录公民对法律及政府项目的投票。此外，市政府还在开发区块链技术的其他用途，计划扩大该项服务的覆盖范围。

2.3.6. 德国

世界首个承认比特币合法地位的国家。2013 年 8 月，德国宣布承认比特币的合法地位，并已纳入国家监管体系。德国银行业协会 Bankenverband（BdB）认为区块链技术可能会对金融市场产生重大影响。2016 年，德国联邦金融监管局（BaFin）对分布式分类账的潜在应用价值进行了探索，包括在跨境支付中的使用，银行之间转账和交易数据的储存。

2.3.7. 日本

日本金融厅（FSA）在 2016 年初提交了议案，关于国内经济管理条例对日本国家立法机关带来的改变。这个定义能让比特币变成一种资产，由此给交易所引进了反洗钱（AML）和了解你的客户（KYC）规则。2016 年 5 月，日本首次批准数字货币监管法案，并定义为财产。日本成立了首个区块链行业组织，叫做区块链合作联盟（BCCC）。该组织由 30 多家对研究开发区块链技术感兴趣的日本公司组成。日本经济贸易产业省（METI）已经发布了有关区块链技术的新调查结果，建议政府“验证使用案例的有效性”。

2.3.8. 澳大利亚

2016 年 3 月，澳大利亚邮政(Australia Post)开始探索区块链技术在身份识别中的应用。澳大利亚邮政计划将区块链技术用于选举投票。维多利亚州和塔斯马尼亚州政府的实体财产主任 Tim Adamson 称，这一系统将做到防篡改、可追溯、匿名和安全。区块链技术在澳大利亚也被应用于政治领域，一个新政党 Flux 正在试图利用区块链技术改写政治通货制度。

2.3.9. 中国

2016 年 2 月央行行长周小川指出“数字货币必须由央行发行，区块链是可选的技术”。此前，央行还召开了数字货币研讨会，央行数字货币的票据原型试点测试成功。

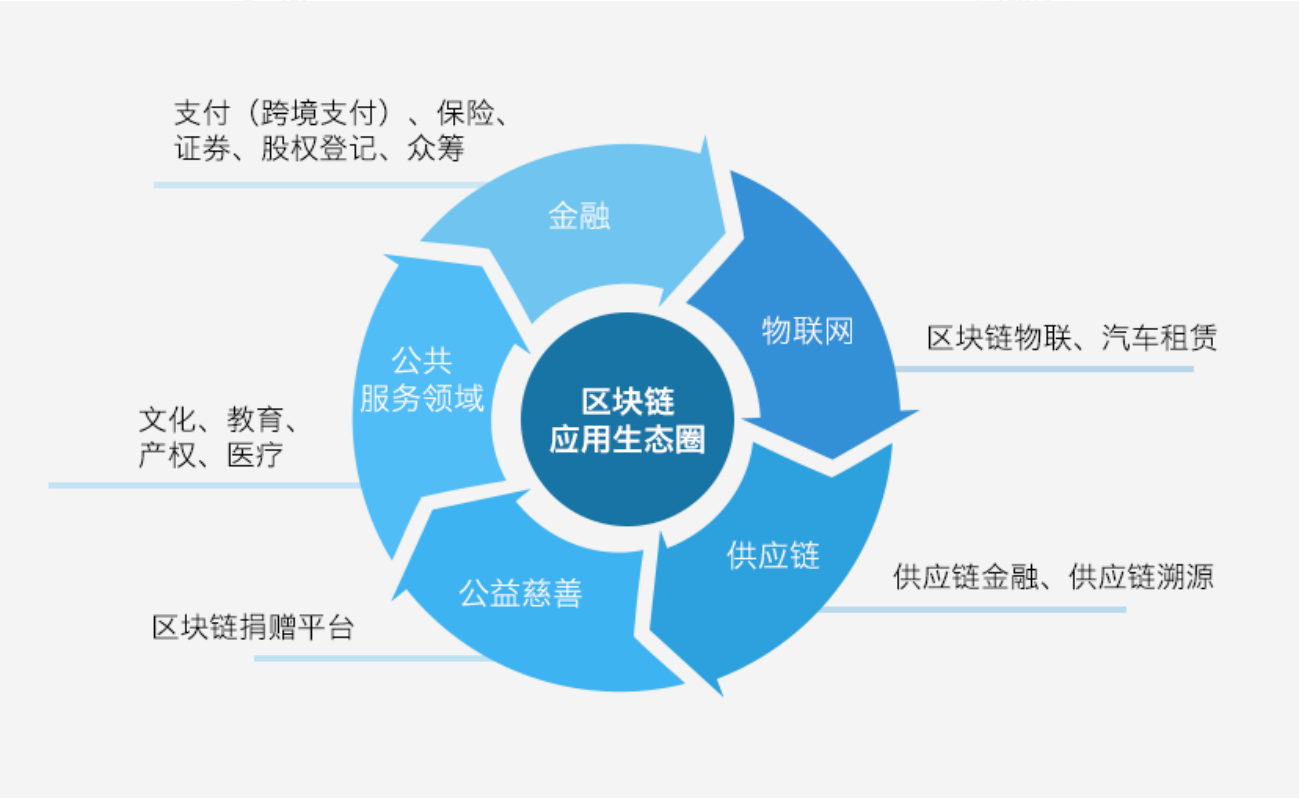
在国务院印发的《“十三五”国家信息化规划》的第四部分重大任务和重点工程中，规划指出要强化区块链等战略性前沿技术并进行超前布局。工信部联合多家知名企业编写区块链技术白皮书，《白皮书》指出了区块链的核心技术路径以及未来区块链技术标准化方向和进程。信通院为此正在密集调研以制定技术标准。

从行业角度来看，一批行业联盟正在建立起来，通过打造区块链的技术、政策、应用的交流平台，推动国内区块链技术的研究和项目落地。2015 年 12 月，区块链研究联盟、区块链应用研究中心成立；2016 年 1 月，全球共享金融 100 人论坛在北京宣布成立“中国区块链研究联盟”;2 月 ,中关村区块链产业联盟成立 ;4 月 ,中国分布式总账基础协议联盟(ChinaLedger)宣布成立。

从企业角度来看，从 2015 年开始，国内陆续涌现了很多区块链技术相关的创业公司。据 Blockchain Angeles 不完全统计，全球共有 1175 家区块链创业公司先后设立，主要集中在美国、欧洲及中国等少数国家地区。据腾讯研究院统计，目前中国共有区块链创业公司及研究

机构近 100 家，其中主要分布在北京，上海，杭州，深圳等经济发达地区，创业企业主要集中在区块链的底层基础架构、数字资产流通、资产鉴证证明、物流、供应链等领域应用。

2.4. 区块链经济发展的重点行业



2.4.1. 金融领域

金融服务产业是全球经济发展的动力，也是中心化程度最高的产业之一。金融市场中交易双方的信息不对称导致无法建立有效的信用机制，产业链条中存在大量中心化的信用中介和信息中介，减缓了系统运转效率，增加了资金往来成本。

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，具备改变金融基础架构的潜力，各类金融资产，如股权、债券、票据、仓单、基金份额等均可以被整合进区块

链账本中，成为链上的数字资产，在区块链上进行存储、转移、交易。使其在金融领域的应用前景广阔。例如，在跨境支付、保险理赔、证券交易、票据等方面有了典型的应用。

在（跨境）支付方面，通过区块链技术，实现资金转移，尤其在跨境支付业务上的潜在优势格外突出，在跨国收付款人之间建立直接交互，简化处理流程，实现实时结算，提高交易效率，降低业务成本，由此推动跨境微支付等商业模式的发展。典型的应用案例是 Visa B2B Connect。国际银行卡组织 Visa 与区块链公司 Chain 共同开发的 B2B 跨境支付项目，计划于 2017 年推出服务，目前已经在 10 个国家的 30 家银行中进行了测试。Visa 和 Chain 联合开发的区块链系统可以实现支付交易的实时处理，从而提高效率，降低成本。

在保险理赔方面，保险机构是传统保险业务的核心，负责资金归集、投资、理赔，往往管理和运营成本较高。通过智能合约的应用，既无需投保人申请，也无需保险公司批准，只要触发理赔条件，实现保单自动理赔，支付理赔金额。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。此外，通过区块链技术，实现个人数据的数字化管理，简化信息认证，有助于更为清晰地披露历史情况。典型的应用案例是 LenderBot,是 2016 年由区块链企业 Stratumn、德勤(Deloitte)与支付服务商 Lemonway 合作推出，它允许人们通过 Facebook Messenger 的聊天功能，注册定制化的微保险产品，为个人之间交换的高价值物品进行投保，而区块链在贷款合同中代替了第三方角色。

在证券交易方面，传统证券业务需中介机构深度参与，才能有效完成股票发行与交易。将股权整合进区块链中，成为数字资产，可实现无需通过中介机构，直接发起交易。资产发行可根据需要，采取保密或公开方式进行。股票资产交易通过区块链代码表达相关各方一致达成的合约，实现合约的自动执行，保证相关合约只在交易对手间可见，而对无关第三方保密。此外，通过相应机制确保证券发行和交易符合监管要求和框架，进一步降低监管合规成本。典型的应用案例是 Linq 平台，由纳斯达克与区块链企业 Chain 合作，于 2016 年 1 月上线的私募股权

交易平台，促进私人股权以一种全新的方式进行转让和出售。。通过 Linq 平台私募的股票发行者享有数字化所有权，同时 Linq 平台能够极大缩减结算时间，降低资金成本和系统性风险。且传统发行和申购材料所需的审批流程也进一步得到简化，提高交易和管理效率。交易方身份、交易量等信息被实时记录在区块链上，有利于证券发行者提高决策效率；公开透明、可追踪的系统有利于证券发行者和监管部门进行市场维护，减少暗箱操作、内幕交易等的发生。

在票据方面，基于区块链技术架构建立新型数字票据业务模式，借助分布式高容错性和非对称加密算法，可实现票据价值的去中心化传递，降低对传统业务模式中票据交易中心的依赖程度，降低系统中心化带来的运营和操作风险。通过区块链的可编程性，有效控制中介市场中的资产错配，借助数据透明特性促进市场交易价格对资金需求反映的真实性，控制市场风险。区块链技术不可篡改的时间戳和全网公开的特性，有效防范“一票多卖”、“打款背书不同步”等问题。

2.4.2. 物联网领域

目前的物联网生态体系，依赖中心化的网络管理架构，所有的设备都是通过云服务器连接。随着网络规模的扩大，中心化云服务器、大型服务器和网络设备的基础设施和维护方面将占用高昂成本。在去中心化的物联网愿景中，区块链是发生互动的设备间促进交易处理和协作的框架，网络上的每个设备都可以作为一个独立、微型的商业主体运行。

2015 年，IBM 与三星联合打造 ADEPT 系统展示了人们在这一方向上的探索：IBM 和三星希望 ADEPT 系统可以让物联网里的各种设备自动运转，从理论上讲，家电的运转出故障时它们可以自动发送信号，并可以自动更新软件。甚至设备本身可以通过 ADEPT 来与周边的设备“沟通”，从而提高能源的利用效率。在 ADEPT 系统中，当数十亿个设备自动交互

信息时，区块链将发挥分布式账本的作用，通过在系统中植入协议，还可以大大降低 ADEPT 系统作为设备间的沟通桥梁时的成本。

此外，Visa 与 DocuSign 联合发起了区块链汽车租赁项目。2015 年 10 月，Visa 与数字交易管理公司 DocuSign 联合推出概念证明项目，使用区块链技术记录、保管租车数据，推动汽车租赁过程的数字化。该项目在区块链上为客户创建数字指纹，在链上进行登记，通过分布式账本记录交易，租车协议、保险项目等内容实时更新，简化传统汽车租赁过程中的繁琐步骤。

2.4.3. 公共服务领域

公共服务是促进经济增长和社会进步的因素，公共服务的供给对政治、经济、社会发展过程中各类主体及制度、文化、态度、行为等都会产生重要影响。传统的公证依赖政府，而有限的数据维度、未建立的历史数据信息链常常导致政府、学校无法获得完整有效的信息。利用区块链可以建立不可篡改的数字化证明。在数字版权、知识产权、证书以及公益领域都可以建立全新的认证机制，改善公共服务领域的管理水平。

文化：利用区块链技术，将文化产业链条中的的各环节加以整合、加速流通，有效缩短价值创造周期。通过区块链技术，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。作品在区块链上被确权，后续交易都会进行实时记录，实现文娱产业全生命周期管理，也可作为司法取证中的技术性保障。数字化证明可以保障数据的完整性、一致性，保护知识产权。例如，Ujo Music 平台借助区块链，建立了音乐版权管理平台新模式，歌曲的创作者与消费者可以建立直接的联系，省去了中间商的费用提成。

教育：利用区块链技术，解决现有的学生信用体系不完整、数据维度局限、缺乏验证手段等问题，简化流程和提高运营效率，并能及时规避信息不透明和容易被篡改的问题。在区块链中记录跨地域、跨院校的学生信息，追踪学生在校园时期的行为记录，构建良性的信用生态体系。此外，通过区块链为学术成果提供不可篡改的数字化证明，可为学术纠纷提供举证依据，降低纠纷事件消耗的人力与时间成本。例如 BitProof 推出区块链学历认证项目。BitProof 是一家专门利用区块链技术进行文件认证的初创公司，该公司与加州软件工程师培训学校 Holberton School 开展合作，利用区块链技术向学生颁发学历证书，实现学历记录真实性。同时通过区块链学历验证体系，招聘者在进行学生背景调查时，通过在线区块链系统，可以快速获得学生学历及毕业证书信息，降低学历伪造风险。

产权登记：目前，房地产交易市场在交易期间和交易后流程中，存在缺乏透明度、手续繁琐、欺诈风险、公共记录出错等问题。区块链技术的应用可实现对土地所有权、房契、留置权等信息的记录和追踪，并确保相关文件的准确性和可核查性。此外，可借助区块链技术实现无纸化和实时交易。例如，美国房地产区块链公司 Ubitquity 研发出适用于房地产行业的文件安全存储区块链平台。从具体的操作上看，区块链技术在房屋产权保护上的应用，可以减少产权搜索时间，实现产权信息共享，避免房产交易过程中的欺诈行为，提高房地产行业的运行效率。

医疗健康：医疗机构面临着无法跨平台安全共享数据的问题。在医疗服务商之间建立良好的数据协作，有助于进一步提高诊断准确率，改善治疗效果，降低医疗成本。基于区块链技术，医疗产业链中的参与方实现对网络访问权限的共享，同时也不会对数据的安全性和完整性造成威胁。此外，随着个人健康数据的不断增长，以中心化方式存储基因、指纹等重要健康数据，一旦发生大规模泄露，将产生灾难性后果。而通过算法确保数据库的安全性，避免单点故障导致数据库整体性崩溃，区块链技术有望为医疗健康行业带来金融级的数据安全保障。例如 Guardtime 医疗档案管理项目。安全初创企业 Guardtime 与爱沙尼亚电子卫生基金会合作，

利用区块链技术保证病人医疗记录的安全。敏感数据保护中存在的安全隐患包含信息篡改、删除、错误升级，区块链技术可以保证数据的真实完整，并能完全记录数据变更过程，从而实现医疗记录和健康档案的实时保护。

2.4.4. 公益慈善领域

区块链上存储的数据，高可靠且不可篡改，天然适合用在社会公益场景。公益流程中的相关信息，如捐赠项目、募集明细、资金流向、受助人反馈等，均可以存放于区块链上，在满足项目参与者隐私保护及其他相关法律法规要求的前提下，有条件地进行公开公示，方便公众和社会监督，助力社会公益的健康发展。例如 BitGive 建设的捐赠平台。BitGive 是一家非营利性电子货币慈善基金会，致力于将比特币及相关技术应用于慈善和人道主义工作中，促进慈善事业发展。2015 年，BitGive 公布慈善 2.0 计划，应用区块链技术建立公开透明的捐赠平台，平台上的捐款的使用和去向都会面向捐助方和社会公众完全开放。

2.4.5. 供应链领域

区块链技术有助于提升供应链管理效率。由于数据在交易各方之间公开透明，从而在整个供应链条上形成一个完整且流畅的信息流，这可确保参与各方及时发现供应链系统运行过程中存在的问题，并针对性地找到解决问题的方法，进而提升供应链管理的整体效率。区块链技术可以避免供应链纠纷。所具有的数据不可篡改和时间戳的存在性证明的特质能很好地运用于解决供应链体系内各参与主体之间的纠纷，实现轻松举证与追责。区块链技术可以用于产品防伪。数据不可篡改与交易可追溯两大特性相结合，可根除供应链内产品流转过程中的假冒伪劣问题。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，提升供应链上信息的透明度和真实性。通过 Provenance 的区块链平台，整合产品制造、运输、交易环节过程中的全部信息，重建供应链条中的信用体系，促进体系的良性发展。

领域	案例	服务商/应用商	时间
跨境支付	Visa B2B Connect	Visa、Chain	2017年（计划）
保险	LenderBot	Stratumn、Deloitte、Lemonway	2016年
证券	Linq	纳斯达克、Chain	2016年
物联网	ADEPT	IBM、三星	2015年
物联网	汽车租赁	Visa、DocuSign	2015年
文化	Ujo Music	Ujo Music	
教育	BitProof	BitProof、Holberton School	
房地产	Ubitquity	Ubitquity	
医疗	Guardtime	Guardtime、爱沙尼亚电子卫生基金会	
慈善	BitGive	BitGive基金会	2015年
供应链	Provenance	Provenance	

第3章. 区块链的世界“军备大赛”

2017 年区块链应用将在全球呈现爆发式增长。就 2016 年发展情形来看，在全球范围内，除比特币以外尚未出现新的成熟区块链应用，中国与全球处于同等水平。而进入 2017 年之后，情形开始有些不同了。2017 年 2 月，美国国会宣布成立区块链决策委员会，将针对区块链技术和数字货币完善相关的公共政策。这标志着行业已经进入监管视野，该机构成立的重要目的在于保护区块链技术不受“过时的监管”所阻碍，意味着行业应用即将进入高速发展期。风险投资家马克·安德森在《华盛顿邮报》的一篇采访中指出，“在 20 年后，我们就会像讨论今天的互联网一样讨论区块链”。

从区块链在北美的发展情况来看，国外金融机构的研究积累比国内多，部分领域有了场景模拟，尤其是在银行业，国外大银行都成立了实验室，科技巨头也推出了各自解决方案。

相比之下，国内缺少足够政策引导。许多项目大都还属于概念验证阶段，主要集中于区块链技术本身学习与研究和应用场景的探索。国内部分银行建立了研发团队，但大多数金融机构通过加入联盟作为探路区块链的开始。部分国内高科技企业在区块链领域已经有了解决方案，距离生产实践只有一步之遥。

3.1. 区块链产业格局

3.1.1. 两条发展路线

面对区块链技术迎面而来的机遇与挑战，全球科技公司、金融公司和咨询公司积极布局，抢占先发优势，大致形成了两条发展路线：

一条是自上而下的路线：代表有大型金融机构，通过组建区块链联盟，寻求合作，探索区块链技术及应用场景，把握行业制高点；亦或是在银行内部的局部领域试点应用，如 UBS、

花旗、德意志银行及巴克莱都成立了区块链实验室，对不同应用场景进行测试，服务于自身业务流程改造。在国内，2016 年年初央行表示将区块链技术作为数字货币的可选技术；中国互联网金融协会成立区块链小组；平安集团和香港友邦保险等机构加入 R3CEV；国内的区块链联盟相继成立。

另一条是自下而上的路线：从比特币到以太坊，社区一直是推动区块链行业发展的重要力量。以一种自成一体的商业模式运作，许多项目选择了 ICO 的方式来融资。

3.1.2. 投资规模倍增

过去几年，区块链行业中的投资金额成倍增加。区块链领域的投资在 2015 年达到了 4.74 亿美元，全球区块链投资事件 65 起，同比增长 43.5%。主要公司如 Ripple、Blockstream、Chain、DAH、Circle 等融资规模超过 5000 万美金。[2]截止到 2016 年 9 月，本年度区块链融资总额达到了 4.9 亿美元。

随着时间推移，区块链领域的投资发生了很大的变化。2016 年以前，投资主要集中在比特币相关的领域，比如矿机芯片、交易平台、支付汇款、钱包服务等。

2016 年以后，区块链作为一个独立领域崛起。考虑到区块链技术在多个领域发展还有极大的不确定性，更多项目集中在底层技术基础架构。不过随着时间推移，行业细分类型越来越多。截止 2016 年 11 月，拿到融资的初创公司超过 200 家，多数处于 A 轮阶段。

除了传统的投资之外，ICO 是区块链行业独有的融资方式，所谓的 ICO 是指通过发行代币的方式来融资。代币代表该项目的一些收益权或股份。项目的支持者可以通过认购相应的价值的代币来投资区块链初创公司。ICO 的另一个不同于传统融资方式的特点是，初创公司往往不会留下很多权益份额，而是把大部分权益份额出让给参与众筹的投资人。

[2]中投顾问产业研究中心《2016-2020 年区块链技术深度调研及投资前景预测报告》

3.2. 国外军团：四大类参与主体

区块链技术与应用在北美、欧洲和亚洲等全球主要市场逐渐受到重视。各类区块链技术和产业联盟先后成立，主要金融机构与科技公司也纷纷加大在区块链领域的布局。

依主体类型区分，参与者包含四类：

1、初创公司或组织：依靠组建跨公司、跨行业领域的国际性区块链平台和联盟来制定行业标准，力求成员间在技术协定、商业应用、监管合规等方面达成一定程度的协同。

2、金融机构：针对已有的应用场景或已知的应用需求，各大传统国际银行通过自研、与外部金融科技公司或其他金融机构合作，实施区块链技术应用试点，建设区块链能力。

3、大型科技公司：大型科技公司和云计算服务商基于 IT 技术开发、云服务等能力，推出区块链相关服务(BaaS, blockchain-as-a-service) ，面向包含金融机构在内的企业客户。

4、咨询公司/系统集成商：整合软件、系统设计与应用、云等 IT 服务的 IT 咨询公司/系统集成商，发展区块链技术与相关服务，以支持金融机构或其他领域企业客户的区块链技术布建与应用。

各类主要代表企业或组织简介如下：

类型	代表企业	优势/特点	案例/方案
初创公司或组织	R3 CEV	以搭建底层技术协议为主	公布源代码的Corda分布式账本
金融机构	高盛	以解决金融机构现有应用场景需求、降低交易成本为主要出发点	银行间清算、外汇交易等
大型科技公司	微软	将原有技术能力（如云服务）延伸至区块链领域	基于Azure云服务，发展莱切利（Bletchley）项目支持不同区块链联盟组建。
系统集成商/IT咨询公司	德勤	结合系统集成能力与区块链技术服务企业客户	基于以太坊的协议的Rubix项目，例如区块链智能身份项目。

3.3. 国内军团：创新活跃

从 2015 年年底，中国真正开始了区块链领域的创新创业。截止 2016 年底，国内已经有近百家与区块链技术相关公司，出现了许多代表性的企业。

在众多的应用方向中，金融行业因雄厚的资金实力成了区块链落地呼声最高的方向。

类型	代表企业	优势/特点	案例/方案
初创公司或组织	万向区块链实验室	搭建开源的技术研究生态及投资孵化生态	基于以太坊的基础设施
Fintech	微众银行	搭建区块链底层服务	清算、票据
大型科技公司	腾讯	将原有技术能力（如云服务）延伸至区块链领域	腾讯金融云+区块链解决方案。用于票据、资产登记及交易等场景。

3.3.1. 国内联盟链发展现状

国内已经形成三大联盟。

受 R3、Hyperledger 等区块链联盟的影响，国内的金融机构不约而同将加入联盟作为探路区块链的第一步，区块链行业始于联盟成立。2016 年 1 月 5 日，中国首个区块链联盟“中国区块链研究联盟”在京成立。2016 年 4 月 19 日，中国分布式总账基础协议联盟（China Ledger）宣告成立。上海证券交易所前总工程师白硕出任了该联盟的技术委员会主任。白硕表示，区块链联盟旨在凝聚中国共识，开垦中国的区块链试验田。5 月 31 日，由微众银行、深金信会、深证通、银链科技等 25 家单位发起的金融区块链合作联盟（深圳）（简称金链盟）正式成立。金链盟中七成是金融机构，三成是金融科技企业和互联网企业。

中国区块链三大联盟

	金链盟	中国分布式总账基础协议联盟（China Ledger）	中国区块链研究联盟（CBRA）
设立目标	在3至5年内研发一条或多条金融区块链，推出多种广受欢迎的区块链终端应用，制定一批高水平联盟标准，申请一批区块链专利技术。	1.聚焦区块链资产端应用，兼顾资金端探索；2.构建满足共性需求的基础分布式账本；3.精选落地场景，开发针对性解决方案；4.基础代码开源，解决方案在成员间共享。	打造区块链技术的研究与交流平台；打造政策沟通平台，厘清区块链技术在现有监管模式与货币政策操作中的定位;打造区块链技术的市场应用平台，推动具体应用规则的规范化、标准化，进行项目落地与路演，形成区块链研究领域具有高端学术品味和较强国际影响力的中国特色新型智库。
成立地点	深圳	上海	北京
设立时间	2016.5.13	2016.4.19	2016.1.5

3.4. 区块链在中国面临的历史性机遇

降成本是历史赋予区块链在中国发展的最大机遇。

2016 年，关于中国制造业综合税负高的讨论引起全社会的关注。降成本是经济社会发展五大任务之一。自十八大以来，从中央到地方先后出台了为企业降成本的措施，政府作了大量工作，从实际情况看，企业需要化解的负担依然较重，降成本还有比较大的空间。

区块链技术是降低企业成本的一剂良药。区块链技术以极低的成本解决了信任与价值的可靠传递难题，具备防伪、防篡改的特性，可以构建一个更加共享开放、更透明可信并可核查追溯的可靠系统，任何数字形式的资产认证、记录、登记、注册、存储、交易、支付、流通，均可通过区块链实现。

首先，区块链技术可以减少违背市场竞争原则和侵害消费者权益的行为，降低企业的搜寻成本、决策成本以及执行成本。

其次，区块链技术有助于削减中介化成本。企业在区块链系统中作为网络上的一个节点，点与点所有点之间都可以直接交易，彼此不需要中介进行信任背书。例如，个人网络消费支付、企业办理年检认证手续、进行各类审核登记等等，都可以通过区块链技术自动完成。

再次，区块链技术有助于降低制度性交易成本。区块链技术有助于削减各种制度性的认证性成本。区块链技术依靠强大的密码学原理构建了一套可信的身份验证的工具，可以建立一套身份识别系统，让企业、产品、应用和服务进行交互。

自主可控、安全可靠则是中国发展区块链需要关注的重要问题。

当前，区块链技术还处于发展的初期阶段，区块链的两个核心技术，即共识算法和加密算法，都存在很大的优化和完善空间。而且，主流的区块链技术平台均发源于国外，如果要运用国外底层平台，还需要花大量时间与精力去改造。我们完全有机会也有必要做一套自主可控的区块链底层平台。

创业者要耐心地从底层技术开发做起，联合创新区块链技术，占领全球区块链的制高点，努力做到区块链技术的自主可控。拥有应用场景的机构要积极拥抱新事物，以开放心态积极与区块链创业者合作。政府对区块链技术的监管政策和鼓励措施都不应过度，一方面应该“让子弹再飞一会儿”，有一定基础之后，再制定监管政策和行业标准，另一方面也要防止一哄而上，拔苗助长。

未来中国区块链的市场规模将有巨大的想象空间。

2016 年起，国内相继成立研究联盟，大多数金融机构迈出了探索区块链的第一步。随着区块链领域的持续升温，2017 年区块链应用落地将进一步加速。同时，中国企业投资海外区块链公司成为趋势，国内公司积极绑定全球资源，形成正反馈效应，带动整个行业发展。

从整体来看，无论从技术标准还是应用场景落地，中国在区块链领域的创新创业活动异常活跃，有望在这场军备竞赛中抢占先机。

第4章. 腾讯区块链方案

腾讯公司在自主创新的基础上，打造了提供企业级服务的“腾讯区块链”解决方案。基于“开放分享”的理念，腾讯将搭建区块链基础设施，并开放内部能力，与全国企业共享，共同推动可信互联网的发展，打造区块链的共赢生态。

腾讯在支付与金融、社交、媒体等多个领域积累了丰富的行业与技术经验，在高并发的交易处理方面取得了业界领先的突破；此外，腾讯还具备海量数据处理和分析、金融安全体系构建的能力，在云生态和行业连接的探索上也积累了丰富的经验。

4.1 腾讯区块链方案的设计原则及目标

腾讯区块链致力于提供企业级区块链基础设施，行业解决方案，以及安全、可靠、灵活的区块链云服务。

4.1.1 设计原则：

自主创新：腾讯区块链注重自主创新，目前在关键领域已经拥有多项自主知识产权的独特核心技术，在共识算法、十亿级用户管理、海量数据并发处理、账户安全管理、风险控制等方面具有专利和技术积累。

安全高效：基于腾讯多年在支付与金融领域的安全、可靠运营经验的积累，推出腾讯可信区块链，能够有效实现信息共享，保护信息安全，提升系统效率。

开放分享：腾讯将搭建区块链基础设施，开放内部服务能力，与行业伙伴共享，共同推动可信互联网的发展，打造区块链的共赢生态。

4.1.2 设计目标：

腾讯可信区块链旨在为行业伙伴提供企业级区块链基础设施，行业解决方案，以及安全、可靠、灵活的区块链云服务。通过高性能的区块链服务，在实现安全可靠的交易对接的前提下，通过可视化的数据管理手段，有效降低企业运营综合成本，提高运营效率。

4.2 腾讯区块整体架构

在“自主创新、安全高效、开放共享”设计原则的指导下，腾讯可信区块链方案的整体架构分成三个层次：腾讯区块链的底层是腾讯自主研发的 Trust SQl 平台，Trust SQL 通过 SQL 和 API 的接口为上层应用场景提供区块链基础服务的功能。核心定位于打造领先的企业级区块链基础平台。中间是平台产品服务层为 Trust Platform，在底层（Trust SQL）之上构建高可用性、可扩展性的区块链应用基础平台产品，其中包括共享账本、鉴证服务、共享经济、数字资产等多个方向，集成相关领域的基础产品功能，帮助企业快速搭建上层区块链应用场景。应用服务层（Trust Application）向最终用户的提供可信、安全、快捷的区块链应用，腾讯未来将携手行业合作伙伴及其技术供应商，共同探索行业区块链发展方向，共同推动区块链应用场景落地。整体框架结构如下图：

图 4-2 腾讯区块链基础框架

4.2.1 底层平台 TrustSQL

用户管理：负责所有区块链参与者的身份信息管理，包括维护公私钥生成、密钥存储管理以及用户真实身份和区块链地址对应关系维护等，并且在授权的情况下，监管和审计某些真实身份的交易情况。对数字资产等金融交易类的应用，还提供了风险控制的规则配置，以保证系统交易安全。

基础服务：基础服务部署在所有区块链的节点上，用来验证业务请求的有效性，并对有效请求完成共识后记录到存储上。对一个新的业务请求，基础服务先对接口适配解析，鉴权处理，然后通过共识算法将交易或者合约加上签名和加密之后，完整一致的存储到共享账本上。共识

机制可自适应，在网络和节点都正常情况下具有高并发性，网络异常或者节点欺骗的情况下具有强容错性。

智能合约：负责合约的注册发行以及合约的触发和执行。用户通过某种编程语言定义合约逻辑，发布到区块链上之后，根据合约条款的逻辑，由用户签名或者其他的事件触发执行，完成交易结算等合约的逻辑。

运营监控：负责产品发布过程中的部署、配置修改、合约设置以及产品运行中的实时状态可视化的输出，如：告警、交易量、网络情况、节点健康状态等。

4.2.2 平台产品服务层 Trust Platform

平台产品服务层抽象了各类典型的区块链应用，提供典型应用的基本能力和实现框架，用户可以基于这些基本能力，叠加自己业务独有的特性，轻松完成业务逻辑的区块链实现。帮助用户快速搬迁已有业务到区块链上，以应对新的场景需求，或者搭建全新的业务场景，利用区块链的不可篡改、防抵赖等特性解决之前难以解决的问题。

数字资产：根据对虚拟货币、游戏装备、商业票据、积分、卡券等数字资产的分析，我们发现资产上链是一个关键环节。为此引入“资产网关”的概念，协助用户进行链下资产到链上资产的转换。资产一旦上链，转移、拆分、提现等操作就会通过帐户公私钥体系严格控制起来，并且所有的操作都会有签名校验，交易双方都会留下痕迹，不可抹除。如商业票据、卡券等存在有效期的资产，还会提供到期自动清算的能力，包括资产发行、资产转让、资产提现、资产清算、资产查询等。

鉴证服务：针对知识产权、保单保全（权益证明）、个人和企业资质证明等应用场景，区块链充分发挥不可抹除和公示的能力，让机构和个人通过一个简单的接口或 APP 客户端就可以把版权资料、投保资料、资质证明等发布到区块链上，让所有记账节点共同为自己作证。另

外基于腾讯自建的知识产权平台，用户的维权将更加方便，证据确认更有权威性。如权属登记、权属注销、侵权证据录入等。

共享账本：金融机构间的对账清算目前基本都是以天为周期进行，对账方式基本也都是互发对账单，对比双方的交易流水。这给最终的交易确认和资金划拨都带来一定的延时，一些需要实时付款的业务场景甚至必须要业务运营方去垫资进行。区块链天然的共享账本，让对账不必第二天汇总发送，而是随时都可以进行，双方只要把对账逻辑对接到区块链上，就可以完成资金的核对。基本可以实现准实时的交易确认和资金划拨，并且任意一方都不可抵赖。特别对于资金链条比较长，牵涉环节比较多的业务非常有竞争优势。同时监管机构也可以参与到共享账本记录中。

分享经济：分享经济能否走的长远，一个关键因素就是供需方之间信任的建立，保证分享行为的顺利实施，而区块链从技术层面提供了一种实现途径。技术保证能力的背书，让彼此难以达成信任的多方参与者，共同建立起公信力，不再需要中间机构或者服务平台构建强大的内部审核流程，严谨繁复的记账备份体系，以及配合监管机构做的额外设施，就可以达到相同的效果。从而节约了大量的成本，让分享更加高效可行。

4.2.3 应用服务层 Trust Application

应用服务层（Trust Application）提供基于区块链方案的应用服务给最终用户的使用。腾讯区块链解决方案中应用服务层将尽力为腾讯的海量用户提供各类区块链场景的服务，未来将在数字票据、贵金属交易、知识产权保护、网络互助、机构清结算、公益等场景为用户提供可信、安全、便捷的区块链服务。腾讯区块链也会本着开放分享的原则，未来将携手各个行业伙伴发掘更多区块链的应用场景，开放区块链底层（Trust SQL）和平台应用层（Trust Platform）的能力，共同开发新的应用服务，一同维护区块链生态。

4.3 底层平台 Trust SQL

4.3.1 基础服务

基础服务模块由接口适配、共识管理，网络通信和记录存储四个部分组成，如下图

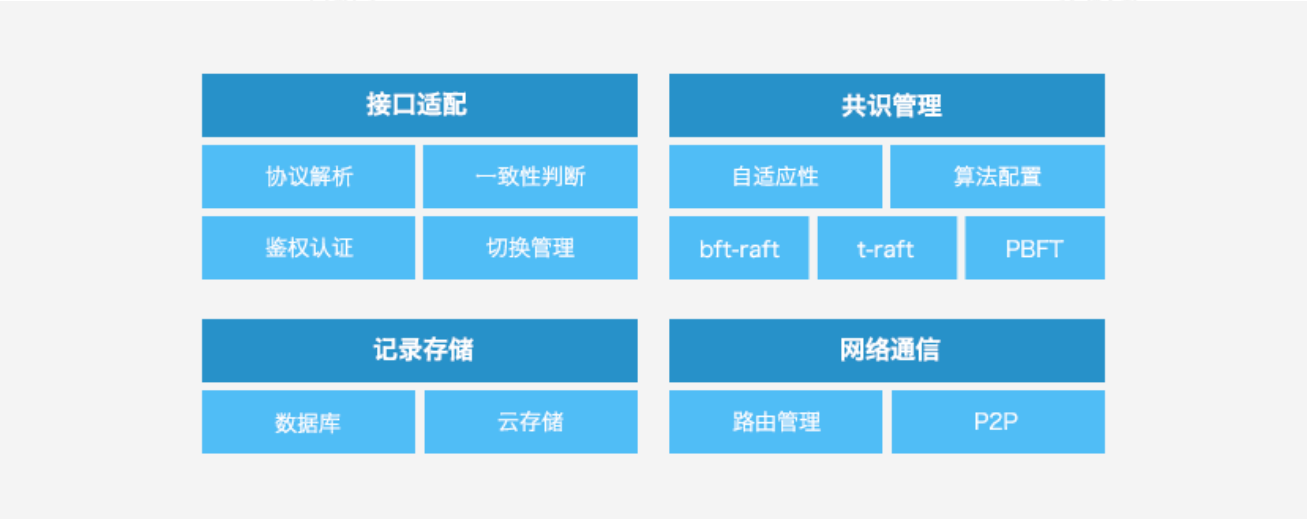


图 4-3-1 基础服务

4.3.1.1 接口适配

为了用户方便、低成本的接入腾讯区块链，Trust SQL 对应用层提供 SQL 和 API 的接口，其中 API 接口支持同步和异步操作两种模式。接口适配层对业务请求进行解析，鉴权和签名校验之后，通过共识算法将业务请求记录到账本存储上。接口适配模块作为共识管理模块的客户端，也会参与共识管理。接口适配模块主要负责各个共识节点返回结果的汇总和一致性判断。另外，当使用具有自主知识产权的“改进的 bft-raft”共识算法时候，接口适配模块还会收到来自业务侧的选举切换请求，接口适配模块对选举切换请求进行汇总统计。当符合切换条件的时候，通知共识管理模块重新选举。

4.3.1.2 共识管理

共识机制是区块链中核心的技术点。多方参与的节点在预设规则下，通过节点间的交互对数据、行为或流程达成一致的过程称为共识。共识机制是指定义共识过程的算法、协议和规则。

共识机制按照共识的过程分两类，第一类是概率一致的共识、工程学上最终确认；第二类是绝对一致之后再共识，共识即确认。腾讯区块链提供第二类的共识机制，支持自适应和用户指定配置两种模式。自适应的模式是在网络状况良好、无欺诈节点的情况下自动使用共识效率高、能够防欺诈的、具有自主知识产权的“改进的 raft”算法，当欺诈节点或者故障节点超过阈值之后自动切换到更为严格的、具有自主知识产权的“改进的 bft-raft”算法。用户指定配置模式是指用户直接配置固定共识机制，进行共识管理。

4.3.1.3 网络通信

网络通信模块负责各节点间以及业务侧的消息数据传输。腾讯区块链采用可以多路复用、连接共享的动态自组织的网络。可以跟现有的防火墙、代理服务器等安全设施很好的兼容，提供点对点的组网和安全可靠的数据传输。

4.3.1.4 记录存储

腾讯区块链记录存储可以支持多种的介质的存储，存储介质可以是数据库、文件系统，也可以是云存储介质，如云 DB，云 KV 等。记录存储采用块链的结构，任何对历史数据篡改都能被自校验发现，并进行告警和自动修正。

4.3.2 用户管理

用户管理主要解决用户身份到区块链地址的映射关系、用户隐私的保密性以及监管审计的可追踪性。从业务场景上看，有些场景是需要匿名、交易不相关性，如股票交易、数字货币等，有些场景则不需要匿名和不相关性，如互助保险、源头跟踪等。要兼顾这两大场景，密钥管理需要很强的适应性和兼容性。腾讯区块链提供了用户灵活自由选择的多种配置方式。

从用户接入的角度看，一种是原有系统改造接入区块链，存在原有安全级别较高的密钥管理体系，如机构清算，银行保理等，另外一种是新应用场景接入区块链或者原有系统没有完善

的密钥管理体系，如一些供应链业务和一些 B2C 业务等。为继承原有安全级别较高的密钥管理系统、同时又能保留原有用户的使用习惯，腾讯区块链提供了传统密钥系统集成、全托管和部分托管三类模式。

传统密钥系统集成：适用于原有私钥系统安全级别较高的用户，如：金融机构、银行原有的 U 盾、电子签名等，对于此类用户，腾讯区块链只需要将原有用户的私钥系统跟区块链地址关联起来即可。

部分托管 :适用于接入区块链服务的部分主体有较高安全级别的密钥系统或者多种区块链技术互通的场景。部分托管情况下，腾讯区块链来保证参与的多方区块链地址关联关系和一致性。

全托管：适合全新接入的场景以及原有互联网习惯程度较高的场景。将原有的以用户名、密码的体系，通过安全的密钥生成和管理系统对应起来，使用户信息跟区块链地址隔离开来，保护用户隐私安全。

对于全托管的模式，腾讯区块链的用户管理系统由账户管理、密钥管理、权限管理和风控审计四个部分组成，如图：

图 4-3-2 用户管理

4.3.2.1 账户管理

账户管理负责用户的账户管理，包括账户的注册、登录、注销以及账户跟密钥的不相关性处理。账户注册时，将原来用户习惯的用户名、密码等身份信息映射到腾讯区块链地址。账户登录之后，才可以发送区块链相关的业务请求。对交易保密程度较高的场景，用户可以选择腾讯区块链地址不相关性处理，使得同一个用户的不同交易在区块记录存储中不具有关联性，提高了用户安全性和交易保密性。

4.3.2.2 密钥管理

在全托管的模式下，密钥管理系统负责用户密钥跟账户的关联、密钥安全管理和丢失找回。用户密钥在客户端生成，用户可以选择将密钥保存在密钥保险箱或者委托给关联账户的方式以便密钥丢失后找回。为了保证用户账户跟密钥关联关系可靠性，密钥管理系统将关联关系的签名采用多节点链式存储。

4.3.2.3 权限管理

权限管理模块负责用户账户、密钥系统、节点加入和退出、数据访问等权限的控制和管理。包括审计权限、账户委托权限、节点共识权限以及用户数据访问权限等。审计权限是为监管机构提供审计的功能，对访问权限和数据范围做严格的控制，对共享账本上交易不相关性的用户可以做到用户关联。账户委托权限用来控制用户账户委托关系的访问控制。共识权限对参与或者新加入节点进行共识权限管理。访问权限用来管理客户端对区块链上的数据查询权限。

4.3.2.3 风控审计

风控模块负责对区块链中数字资产类的交易行为进行风险控制，腾讯区块链提供风控专家模型系统，通过分析和捕捉海量数据间的深层关系，自适应调整风控规则，及时发现风险、管

理风控和控制风险，做到防患于未然。审计模块为审计机构提供审计能力，通过严格的权限控制来保证审计能力只能被审计机构使用。

4.3.3 智能合约

腾讯区块链合约部分包括标准合约以及业务定制的合约两种类型。标准合约包括资产一致性检查、自动成交撮合、多方共同确认的转账、到期自动清算等逻辑相对简单的合约，是腾讯区块链内置合约，可以直接挂在区块链上使用。用户定制的智能合约包括通过合约模板修改配置和添加其他业务逻辑的形式，也可以支持更加复杂的用户自编程的合约，在独立的环境里运行。

智能合约包括合约的注册、触发、执行以及注销四个部分，如下图：

图 4-3-3 智能合约

4.3.3.1 合约注册

合约注册是将用户编写好的合约安全检查处理之后，共识存储到区块链的过程。腾讯区块链未来计划支持多种语言来编写智能合约。

4.3.3.2 合约触发

合约触发是在合约注册之后，通过外部条件来触发合约执行的过程，支持定时触发、事件触发、交易触发和其他合约触发的方式。定时触发是指满足合约中预设的时间之后，节点就触发时间共识之后，自动触发合约调用的过程。事件、交易和其他合约调用都是一次新的请求共识过程中触发合约执行。

4.3.3.3 合约执行

合约执行是合约代码在独立的环境中运行的完整过程，包括对合约构造镜像环境、代码执行、执行代码中状态修改的共识以及共识的异常处理。

4.3.3.4 合约注销

合约注销，是对已经执行过、过期作废或者业务需求变更不再需要的合约进行转存，清理，清理的过程需要多节点共识之后才能完成。

4.3.4 运营监控

为了客户快速接入以及接入之后能够快速准确地识别系统的运行状态以及在运行中满足其他的运维需求，如存储账本扩容、程序升级等。腾讯区块链提供了完整、快捷、可视化的运营监控系统，运营监控主要包括配置，监控、告警、发布和业务分析等功能。

4.3.4.1 配置

负责处理网络节点的相关配置，如共识算法的选择、自适应阈值、存储账本的存储方式、网络路由方式等，配置的本身可以作为区块链中的一个交易的形式下发，通过共识算法达成一致之后再生效。

4.3.4.2 监控

负责收集系统中运行的状态数据，并且可视化的呈现出来。系统中的状态数据包括系统的访问量、耗时、节点的健康状态以及比较底层的机器资源（CPU、内存、硬盘）使用状况等，通过可视化监控可以实时了解整个区块链系统的状态。

4.3.4.3 告警

对系统中比较严重的情况如欺诈节点、账本篡改、机器故障等情况通过短信、电话、微信、邮件等方式通知到相关人员，以便及时处理。

4.3.4.4 发布

对系统初次部署、运行中程序升级以及运行过程中节点扩展等场景下的操作可以通过发布模块来支持。发布模块保证接口、共识算法等重要模块的可执行程序的一致性。

4.3.4.5 业务分析

业务分析包括各个节点间数据一致性检测以及交易数据多维度的统计和分析，可以给特定授权用户提供业务统计分析以及业务发展趋势的图表。

4.3.4.6 云适配

云适配提供目前云主流运营商的接口适配，可以让腾讯区块链更加方便的部署在云上，方便维护和扩展。

4.4 技术特色和优势

在“自主创新、安全高效、开放分享”的设计原则下，腾讯区块链打造的企业级基础设施服务，具有如下特点：高性能、高安全性、高速接入、高效运营：

1、高性能：依托腾讯支付的海量并发经验，交易支持秒级确认；提供海量数据存储，具备每秒万级的处理能力；

2、高安全性：提供丰富的权限策略、安全的密钥管理体系和用户隐私保密方案，保障数据安全。

3、高速接入：丰富的应用开发框架和灵活的部署方式，方便不同类型的用户快速接入，构建应用；

4、高效运营：提供全面、实时、可视化的运维管理系统，快速识别系统状态，满足多个层级的运营管理需求。

4.4.1 高性能

4.4.1.1 丰富的高并发处理经验

腾讯支付基础平台与金融应用线（FiT）现有系统在 2017 年春节红包期间每秒处理超过 20 万的并发交易，腾讯区块链借鉴了 FiT 高并发、分布式账户管理的经验，通过各种模型分析、压测，可以支持每秒万级的处理能力。

4.4.1.2 高效自适应共识算法

在企业级区块链解决方案中，单个区块链的并发处理的能力主要受制于共识算法。实际的联盟链应用中，绝大部分时间里，各节点间网络状况是良好的，节点故障或者是拜占庭节点的概率小，这样，在绝大部分时间里，只需要解决多个节点数据一致性，高效完成交易即可。只要在发现有节点故障或者欺诈的时候，能够自动切换到具有拜占庭容错的算法就可以保证业务顺利进行。腾讯区块链提供的自适应的区块链共识算法，在网络状况良好、无节点故障或者欺诈的情况下处理效率很高，并且可以准确检测节点故障或者节点欺诈；当检测到节点故障或者欺诈，系统自动启用拜占庭容错的算法特性，在总节点数为 3f+1 的网络中（其中 f 为拜占庭错误节点数），当容错节点不超过 f 的情况下，系统正常对外提供服务；当所有坏节点修复或

者拜占庭容错节点解决之后，所有节点数据能全一致的时候，自动切回到高效的算法上。自适应算法很好保证联盟链绝大部分时间内高效的并发处理，并且精准处理了节点错误的问题。

4.4.1.3 交易快速确认

腾讯区块链采用高效自适应的共识算法，保证了共识完成即交易确认，并且对交易确认过程中的其他环节，如签名算法、账本存储方式等进行了优化，实现了秒级确认交易。

4.4.1.4 海量存储

腾讯区块链支持本地数据库存储、文件系统存储以及云存储多种方式。本地存储实现冷热分离，数据库存储使用分库分表的模式，云存储支持按照云的集群规则扩展。

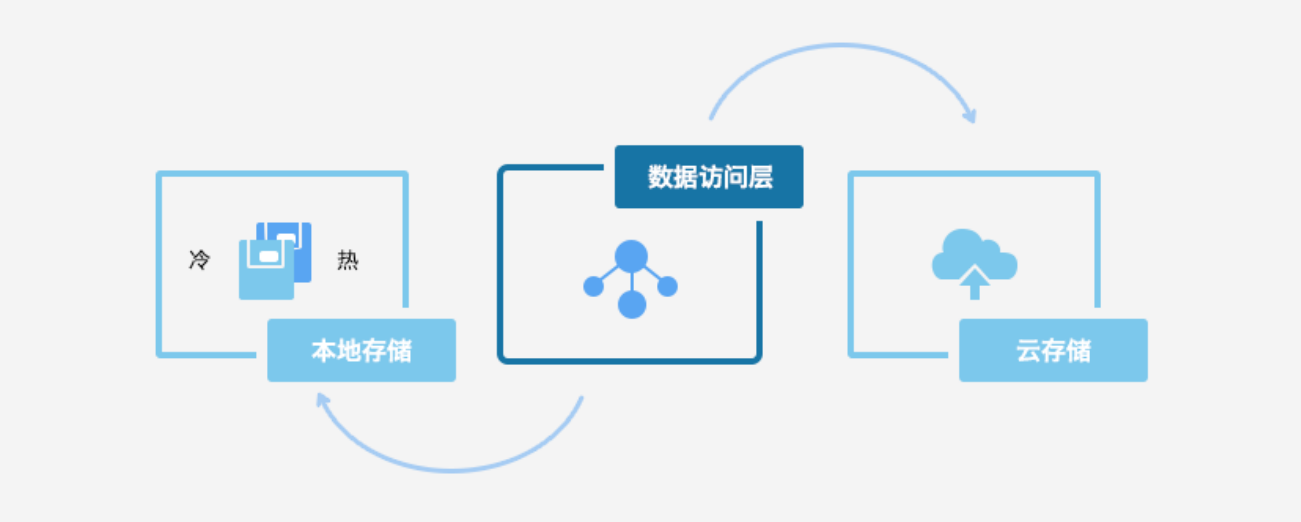


图 4-4-1-4 海量存储

4.4.2 高速接入

在实际的业务对接场景大致分为三类：第一类，原有系统改造后接入区块链，第二类，原有系统上新的需求使用区块链开发，第三类，在全新的系统和场景使用区块链。

腾讯区块链为了适应于上述三类场景，本着业务开发工作量尽量少、尽量满足用户原有开发习惯、方便的部署、保持原有的安全体系的原则，在用户业务开发方式、部署方式以及安全

性继承上做了大量的兼容性设计，可以实现各种场景、各种开发习惯的用户能以较低的代价、较快的速度对接到区块链上来。

4.4.2.1 满足多种用户习惯的方式接入

腾讯区块链平台产品层（Trust Platform）提供丰富的应用开发的框架，应用类型包含了数字资产、共享账本、鉴证证明、股份众筹及所有权交易等基本应用模型。用户可以基于这些应用开发框架进行业务开发，也可以直接基于腾讯区块链底层 Trust SQL 提供的 SQL 和 API 进行开发。对业务开发中使用的底层 API 的库提供了多语言支持，可以满足不同的用户的开发习惯，降低用户接入难度。

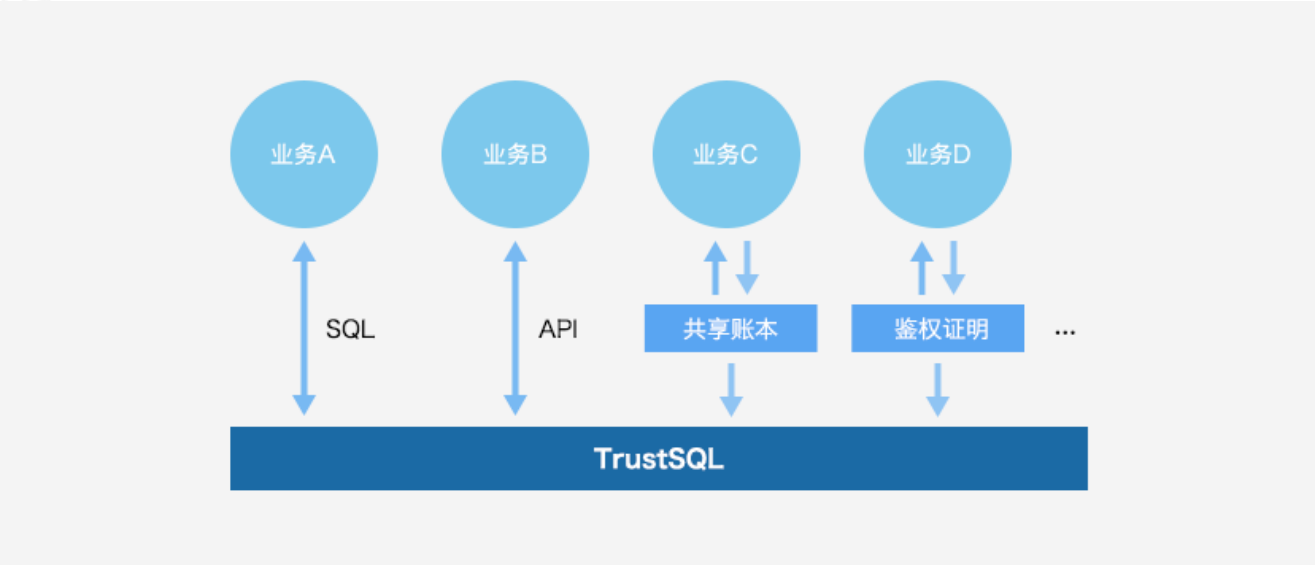


图 4-4-2-1 海量存储

4.4.2.2 跨平台的部署方式

腾讯区块链针对不同的用户需求，可以支持云部署、服务器部署等多种部署方式，适应多种用户部署环境。

4.4.2.3 可选的密钥管理对接机制

腾讯区块链提供了原有密钥系统关联、部分托管和全托管三类对接机制，跟现有系统对接时，可以根据现有系统的密钥管理系统的实际情况选择合适的对接机制。原有密钥系统安全程

度较高的，可以复用的直接使用原有密钥关联的方式；全新的业务可以选择密钥管理全托管的方式；也可以根据业务情况选择部分托管的方式。

4.4.3 高安全性

4.4.3.1 可靠一致的记录存储

腾讯区块链通过非对称加密的数字签名保证业务请求在传输过程中不能被篡改，通过共识机制保证各节点的数据一致的存储。对于已经存储的数据记录通过节点内的自校验性和准实时多节点数据校验来保证已经存储的数据记录不能被修改。

节点的自校验性：腾讯区块链采用块链结构存储数据记录，其中部分记录的修改会破坏块链结构的完整性，可以快速校验出来并从其他节点将数据恢复。另外腾讯区块链每个记账节点都有自己的私钥，每个区块头中包含了本节点私钥的签名，区块内数据的修改都可以通过签名校验出来。

多节点准实时的数据校验：当节点的私钥被盗取，恶意用户是存在修改账本链上所有数据的可能性的，腾讯区块链提供了多节点间准实时的数据对比机制，可以及时发现某个节点账本数据被篡改的情况。

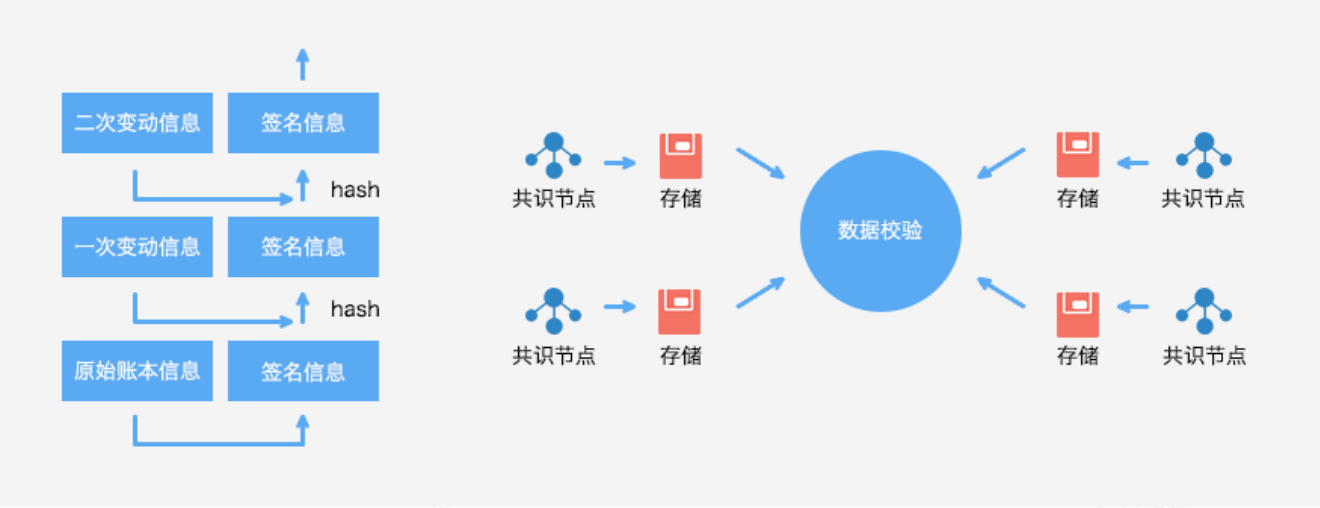


图 4-4-3-1 海量存储

4.4.3.2 用户隐私和交易保密

腾讯区块链中用户信息和区块链地址是隔离的。从各节点的记录存储中，无法获取到相关联的用户信息。用户信息存储有权限控制，访问认证，加密存储等多层保护。对交易保密程度较高的用户还可以选择交易不相关性机制，同一个用户的每次交易都映射到区块链上不同的地址上，从而保证了在交易账本上无法获取一个用户的多笔交易的关联性。

4.4.3.3 安全的密钥管理体系

在腾讯区块链的密钥管理解决方案中，提供了密钥保险箱和用户账户委托的功能来保证密钥的安全。密钥保险箱使用用户信息对密钥加密并分割存储在多个不同的节点上，正常业务流程下不会访问密钥保险箱，当用户密钥丢失后，可以通过对用户信息认证之后将密钥找回。账户委托是通过委托账户来操作被委托账户来实现账户找回的功能，腾讯区块链所有委托账户操作会独立记录在区块链上，并且对委托账户的操作有严格的频度限制和独立的风控策略，可以严格控制委托账户的操作风险。

4.4.4 高效运营

腾讯区块链实现了可视化的服务交付和可视化的服务度量。在服务交付方面，从代码编译、测试、灰度环境验收到正式环境部署，整个服务交付流程实现可视化管理。在服务度量方面，对数据进行了标准化的分层归类，从基础设施、上层组件、应用服务、到用户侧，基于应用的拓扑架构，收集各类指标，统一到一个分析平台中展现。

腾讯区块链提供通用高效的信息采集组件，部署在业务层、共识节点层以及账本存储层，信息采集组件把机器的系统信息（如，CPU，内存、硬盘、网络等状态）、节点使用状态（如

节点访问量、访问时耗、节点健康状态等）以及业务使用情况（业务访问量、成功率、耗时分布等）实时展示到监控界面上，便于整个系统的管理。

4.5 行业应用前景

我们注意到，区块链技术已在世界各地呈现方兴未艾的发展态势。从业务上看，借助区块链的安全特性与信任机制， 将成为发展数字经济的重要技术引擎，可以在多行业领域发挥作用，行业应用领域发展潜力巨大。但从行业 IT 系统需求的角度来看，要在区块链上构建应用，需要区块链解决方案具备强大的三个底层能力：一是完善的新旧系统兼容/切换能力，二是全新的系统安全能力，三是适用多场景的用户隐私保护能力。

基于上述需求，腾讯区块链提供了高可用性、可扩展的区块链应用基础平台，通过此平台，各领域的合作伙伴可以快速搭建上层区块链应用，帮助企业将精力聚焦在业务本身和商业模式的运营上，让用户、商户、机构在多样化的应用场景中受益。

4.5.1 腾讯区块链应用场景概览

基于腾讯区块链基础平台，区块链技术的应用范畴，可以涵盖货币、金融、经济、社会的诸多领域。从区块链应用价值角度出发，我们总结腾讯区块连方案使用场景方向，具备分为：鉴证证明、共享账本、智能合约、共享经济、数字资产等五大类，具体场景概览示意如下：

图 4-5-1 腾讯区块链应用场景

4.5.2 腾讯区块链应用落地中常见问题

Q1：去中心化的特性是否对中心化机构不利？

A1：区块链虽有去中心化的特性，但很多线上业务的纠纷无法离开中心来解决。因此区块链的真正价值在于促进各行各业的中心化机构之间达成共识，构建联盟，形成多个中心组成的商业生态圈，这样的生态系统突出了中心的职能，大大简化了中心化机构运营成本。

Q2：区块链是低效服务吗？

A2：区块链服务是低效是一个认识上的误区。区块链的效率瓶颈主要在于共识算法，而共识算法在不同场景下有不同的实现方式。例如腾讯区块链采用自主研发的高效自适应共识算法，保证了共识完成即交易确认，并且对交易确认过程中的其他环节，如签名算法、账本存储方式等进行了优化，实现了秒级确认交易。

Q3：区块链是否没有隐私？

A3：区块链通过多重的隐私保护方案来保护用户隐私。底层交易数据通过加密方式存储，仅对用户本身可见；上层应用通过严格的权限控制确保隐私安全。

Q4：如何寻找适合区块链适用的场景？

A4：成熟的腾讯区块链解决方案可满足多场景的应用，从具体行业应用适用性考虑，可以综合参考行业各参与方的信任机制、信任内容、业务角色、业务关系、运作方式等维度，通过下图所示，用雷达扫描法进行场景匹配考量。

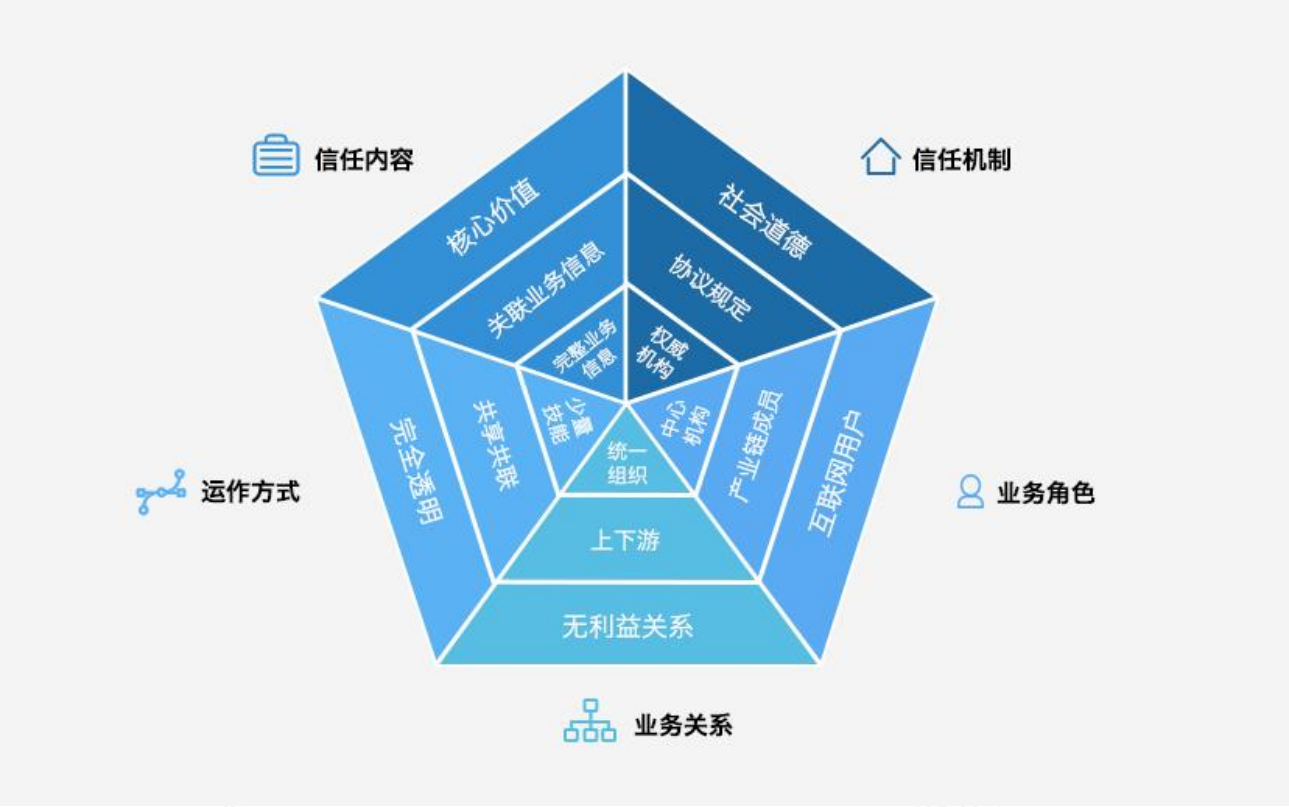


图 4-5-2 腾讯区块链应用场景雷达扫描图

-

第5章. 领导未来

减少欺诈，降低成本，提高效率，这是区块链技术的突出优势。区块链技术的广泛应用，必将加速“数字化信用社会”的到来，势必引发政府管理形态和社会公信力的变革。我们认为，政府参与区块链的发展和监管非常有必要，应该鼓励对区块链技术的深入研究和区块链应用的不断实践。

区块链将成为构筑数字化信用的基石。如果将之用于公益捐赠，每一笔款项都会记录在区块链上，没有营私舞弊的空间。如果将之用于防伪打假，每一个产品都可以溯源而相关交易都有记录，进而消除了造假的空间维护了市场正义。如果企业或某一组织，将之用于薪酬发放，那么各行各业或将不存在劳资纠纷问题。

纵观全球发达国家，已经加入区块链的“军备大赛”。政府应考虑将区块链纳入国家发展战略，积极参与全球竞争，成为大时代的领导者。

正如任何一次技术革命都会带来一些新的问题，区块链的发展遇到的挑战是如何建立能够促进该技术应用的监管环境，如果套用传统的监管模式，会极大的遏制创新，无法发挥其应有的潜力。因此，迫切需要政府的管理理念实现由“监管”到“治理”的转变，基调应当是鼓励创新，同时守住底线。

为有效推动我国区块链技术和应用发展，培育形成具有全球竞争力的区块链产业，提出以下建议：

1、加强区块链技术的安全研究

尚未成熟的区块链技术，从安全性分析的角度，面临着算法安全性、协议安全性、使用安全性、实现安全性和系统安全性的挑战，前不久发生的以太坊自治组织 The DAO 众筹资金被

劫持事件，以及 Bitfinex 交易所比特币被盗事件，暴露了区块链应用上的安全问题。因此，要加强对加密技术、密钥存储、隐私保护、技术实现等方面的安全研究，努力提高区块链技术的整体安全可靠水平。

2、鼓励核心关键技术攻关，形成自主创新体系

鼓励国内重点企业、科研机构、高校等加强合作，加快对共识机制、可编程合约、分布式存储、数字签名等核心关键技术的攻关，争取形成具有我国自主产权的技术成果，打造更加符合国家安全要求的完全自主可控的区块链平台，为众多应用的发展与落地保驾护航。

3、推动形成区块链应用发展的良好环境

面对区块链这类颠覆性技术，虽然在个人隐私和消费者保护、伦理和社会影响等方面面临挑战，但这些挑战最终都将会被解决，因为互联网就是一个很好的先例。因此，建议相关部门加强沟通协调，集聚产学研用等多方资源，密切跟踪国际产业发展前沿动向，通过多种形式共同推进区块链相关理论研究、技术研发、应用推广等工作，优化区块链技术产业的发展环境，力争在新一轮的产业竞争中取得先机。

4、出台扶持区块链技术和应用发展的政策

借鉴发达国家和地区的先进做法，结合我国区块链技术和应用发展情况，及时出台相关扶持政策，重点支持核心关键技术攻关、行业应用解决方案研发、重大应用示范工程、公共服务平台建设等。同时，放宽市场准入限制，加强事中事后监管，优化服务水平。

5、加快推动区块链领域的标准体系建设

围绕产业发展的重点环节，加快推进关键急需标准的部署和制定工作，逐步完善区块链技术和应用标准体系。积极参与国际标准研制工作，对接国际化标准机构和开源社区组织，加强国际交流合作，在积极做出贡献的同时，不断提升我国标准工作的国际话语权。

6、加速推动区块链技术的应用落地

建议围绕金融、文化、医疗、教育、物联网、供应链等行业的典型应用需求，研究提出区块链行业应用解决方案。面向基础条件好、示范效应强的行业领域，探索组织开展区块链应用试点示范工作，推动区块链技术和行业应用的融合发展。

7、加强国际国内交流与合作

鼓励和支持国内企业积极参与国际区块链开源社区，贡献力量，提升影响力和话语权。鼓励学习借鉴国际开源社区建设和运营模式，加强国内企业间的合作，建设我国区块链开源社区，围绕核心关键技术攻关、行业应用解决方案研发、重大应用示范、标准制定等，开展交流与合作。

参考文献

1、《区块链：定义未来金融与经济新格局》，张健，机械工业出版社；

2、《区块链：将如何重新定义世界》，唐文剑，吕雯，机械工业出版社；

3、《区块链革命：比特币底层技术如何改变货币、商业和世界》，唐·塔普斯科特、亚力克斯·塔普斯科特著，中信出版社；

4、引自 2016 年 9 月 1 日，未央网，胡宁《全球政府区块链技术应用一览》；

5、引自 2016 年 11 月 28 日，凤凰财经 WEMONEY《区块链应用的经济学原理》；

6、引自 2016 年 8 月 1 日，新浪财经，徐利《各国政府对区块链都持何种态度？》；

7、《中国区块链技术和应用发展白皮书（2016）》，工业和信息化部信息化和软件服务业司；

8、《分布式账本技术：超越区块链》，英国政府首席科学顾问报告，万向区块链实验室编译；

9、《中国区块链技术和应用发展白皮书（2016）》，工业和信息化部信息化和软件服务业司；

10、 《英国将区块链列入国家战略部署，并制定详细战略实施规划》，2016-05-13 ，蔡维德、赵精武，中国信息化百人会；

11、 区块链铅笔， chainb.baijia.baidu.com；

12、 Blockchain Technology Market by Provider, Application, Organization Size, Vertical, and Region - Global Forecast to 2021, MarketsandMarkets, October 2016；

13、 《The future of financial infrastructureAn ambitious look at how blockchain can reshape financial services》，world economy forum，August 2016；