

华为区块链白皮书 2021

建设融合开放的数字经济基础设施



2021年9月

前言

区块链被业界认为将是颠覆互联网的技术，变革传统的生产关系、提高生产力的创新体系，21世纪最伟大的技术革新，亦是未来网络信息和数据资产交换和流通的必要基础设施。但是这一基础设施的建设并非易事，需要我们聚焦区块链底层核心技术与系统的研发，使得区块链系统更加易用、稳健和高效；同时我们也需要理清数字经济发展的新需求，从而通过构建与之匹配的设施来服务社会与经济部门。

区块链自2008年以来，经历了三个发展阶段。第一个阶段（2009年-2018年），区块链从原有的虚拟货币应用逐渐趋向于实体经济应用，原有的币圈与链圈的炒作，也以链为发展方向而逐渐明晰。第二个阶段（2018年-2020年），区块链以行业应用和服务民生应用为方向，并衍生出一系列适合不同场景的技术方案。在应用场景上围绕数字政务、金融、医疗、版权、工业、环保等主要行业开展应用试点，因此这一时期也出现了众多的区块链技术平台，也由此带来因多链带来的业务被割裂，多链难以互通的产业新问题。第三阶段（2020年-至今），区块链需要避免孤立，打通单链孤岛，实现业务间的可信互通。由此我们可以看出，区块链一方面在加速技术自身的深度发展，夯实其作为基础设施的能力；另一方面需要围绕业务以端到端流程为根本，保障业务流、信息流等多流场景的端到端可信问题。

近年来，区块链技术通过不断地探索、试错已形成三点基本的产业共识：其一、区块链天生具备分布式与联盟属性。区块链依托这一属性围绕参与方共同的交易目标，实现可信的交易。其二、区块链在改变当前的交易模式。原有的交易模式以实物抵押或第三方担保的模式开展交易，虽然这种模式在IT时代对业务发展有益，而在DT（Data

Technology) 时代, 社会经济和新一代信息技术的发展要求更加高效敏捷的交易模式, 原有模式的误差性在增大, 弊端在不断呈现。而区块链以数据为核心构筑可信交易模式, 缩短需求和信息的传递链, 支撑数字经济发展新需求。其三、区块链以服务行业为重点, 作为数字经济基础设施赋能千行百业。行业发展的根本是数据, 原有的数据是以“数据湖”或“数据池”的方式无法“浇灌”行业流程中的分支末节, 区块链在构筑数据要素安全流转的“数据河”, 通过可信流转服务行业, 从而实现行业服务数字经济发展目标。

DT时代的到来, 消除信息孤岛已成为各界的共识, 区块链依托其主要特性, 防篡改、可追溯和可编程等, 通过联盟节点平权共治的方式逐渐形成多中介化的组网模式, 并以区块链技术为核心, 融合其他技术, 如: IOT、5G、数据网络、云计算、大数据、AI以及今后的量子加密等, 形成一体化融合开放的区块链系统架构, 围绕数据端到端可信流转, 解决传统集中模式下数据不敢、不能、不愿共享的问题, 加速数字经济产业发展的进程。

新的时代要求区块链技术和理念与之匹配并不断演进, 我们因此深知区块链仍然存在巨大的发展空间。明天的变化速度可能比今天变化更快, 我们唯有不断创新, 保持领先, 通过构建融合、开放的区块链基础设施, 才能为数字经济建设和高速发展奠定坚实的基础。

编委会成员

顾问： 张文林、肖然、徐峰、谈宗玮、谭焜、陈威、祁峰、赵志鹏、俞岳、钱骁

撰写（按拼音排列）： 曹朝、杜明晓、何超、刘再耀、宁军、郭凯、曲强、孙雪

梅、王磊、徐霆、薛腾飞、杨锐捷、张小军、张子怡、张亮亮、张衡

审稿： 张小军、曲强、张子怡、王磊、刘再耀、何超、张亮亮

目 录

前言.....	1
1. 数字经济驱动下的区块链产业新变化.....	7
1.1 全球区块链新变化.....	7
1.1.1 全球区块链产业政策的变化方向.....	7
1.1.2 全球区块链产业标准的变化方向.....	9
1.1.3 全球区块链的技术发展动态.....	11
1.2 新形势对区块链的需求.....	12
2. 华为区块链作为基础设施的技术与方案特点.....	13
2.1 华为区块链发展思路及方向.....	13
2.1.1 华为区块链发展史介绍.....	13
2.1.2 华为区块链目标：深耕联盟链核心技术，愿做数字经济的筑基者 ...	14
2.2 华为区块链的技术特点.....	16
2.2.1 华为区块链的技术架构.....	16
2.2.2 华为区块链关键的核心技术.....	20
2.3 华为区块链 APaaS 服务栈.....	32

2.3.1 可信分布式数字身份服务(TDIS)	32
2.3.2 可信数据交换与计算服务(TC3)	34
2.3.3 可信跨链数据链接服务(TCDAS)	35
3. 华为区块链的典型应用实践	37
3.1 城市大数据可信共享枢纽—目录区块链	39
3.1.1 背景：基于区块链实现政务数据的统一调度、管理和控制	39
3.1.2 痛点：解决数据共享难问题	40
3.1.3 方案：依靠区块链实现数据可用不可见，可见不可得	41
3.1.4 成效：提升智慧政务效率，增强民生服务体验感	44
3.2 医疗健康——基于区块链的医联体	45
3.2.1 背景：医疗机构与健康保险机构数据拉通是关键	45
3.2.2 痛点：数据不安全、信息孤岛等制约医疗健康及医保体系	46
3.2.3 方案：构筑可信区块链医疗平台，打通医疗数据提升幸福感	46
3.2.4 成效：晚上医疗救助体系，增强全民健康指数	49
3.3 智慧金融——区块链的供应链金融	50
3.3.1 背景：供应链环节多，环节出差将导致重大损失	50

3.3.2	痛点：信息不通，合同造假等导致集中模式下确权难.....	51
3.3.3	方案：借助区块链实现信用穿透助力供应链企业融资.....	51
3.3.4	成效：降低供应链金融风险，提升集团供应链企业的稳健性.....	54
4.	华为区块链的发展展望	55
4.1	华为对区块链的产业展望.....	56
4.2	华为对区块链的技术展望.....	58
4.2.1	区块链自身技术的发展趋势	58
4.2.2	区块链与周边技术深度融合	61
5.	总结.....	64

1. 数字经济驱动下的区块链产业新变化

数字经济是借助对数据要素的识别、选择、过滤、存储和使用的一整套以实现资源的快速优化配置与再生、实现经济高质量发展的经济形态。数字经济在技术层面利用大数据、云计算、物联网、区块链、人工智能、5G 通信等新兴技术，构成以数据为核心的新经济应用形态。

区块链是数字经济时代的产物。目前全球正快速进入数字经济时代，各行各业都在数字化，在此过程中区块链帮助数字资产实现可信流转。未来区块链数量将成为数字经济发展的指标，区块链的内核技术、融合能力和开放能力将是数字经济发展的基础能力。

1.1 全球区块链新变化

1.1.1 全球区块链产业政策的变化方向



图 1-1. 全球区块链产业政策概览图

美国：

目前美国绝大多数州政府已明确对区块链技术的监管立场，很多州政府已制定或颁布区块链领域相关法律。其中亚利桑那州、特拉华州、伊利诺伊州等认为区块链在美国的经济中将发挥重大作用。2020 年 10 月美国政府公布了“国家关键技术和新兴技术战略”将区块链纳入管制技术，美国需要发展这些新技术以保护国家基础设施的安全。

欧洲：

欧洲对区块链总体持欢迎态度。其中德国政府对于区块链的态度积极，德国柏林被称作欧洲区块链蓝海中心。德国政府一方面扶持创业企业，另一方面探讨区块链项目的合规问题。2019 年 9 月 18 日德国联邦政府审议通过并发布“德国区块链战略”，明确区块链国家战略，德国认为区块链技术未来是互联网的组成部分，可以有效助力德国数字经济的发展。

中国：

中央政府从区块链出现之初，一方面规范其合法性发展，另一方面加速区块链的技术和应用创新。伴随着区块链的蓬勃兴起，国家及相关部委不断加大对区块链的引导力度，逐渐明确对区块链的定位。2016 年 12 月 27 日印发的《“十三五”国家信息化规划》中首次将区块链纳入其中。2018 年 5 月 28 日，习近平总书记在中国科学院第十九次院士大会、中国工程院第十四次院士大会上的讲话中首次提到区块链技术，并将其定位为新一代信息技术。2019 年 10 月 24 日，习近平总书记在中央政治局第十八次集体学习时强调，把区块链作为核心技术自主创新重要突破口，加快推动区块链技术和产业创新发展。

展。工业和信息化部、中国人民银行、教育部等多部门将区块链融入相关的产业领域或发展战略，推动行业应用发展。2021 年《中华人民共和国国民经济和社会发展第十四个五年规划和 2035 年远景目标纲要》中将区块链纳入七大数字经济重点产业之一，及工信部和中央网信办联合发布《关于加快推动区块链技术应用和产业发展的指导意见》明确区块链要发展联盟链，要关注底层技术研发，要围绕民生应用推动场景落地。这些政策推动区块链在中国快速进入落地期。

1.1.2 全球区块链产业标准的变化方向

变化 1：全球区块链标准工作进入高速发展时期

区块链的标准化工作始于 2016 年，目前越来越多的国际标准组织，国家标准组织和行业标准组织在积极开展标准制定工作。近两三年区块链标准化发展迅速，无论是从深度（区块链通用技术标准细化程度）和广度（区块链涉及的行业应用标准覆盖范围）都比以前有明显的提升，区块链标准化工作已进入高速发展期。

国际电信联盟标准化组织 ITU-T 早在 2016 就启动了区块链标准化工作。2020 年国际电信联盟第十六研究组 ITU-T SG16 新成立分布式账本技术与应用工作组（Q22）开展基于分布式账本技术的参考架构，跨链、测试与评估、监管等方面标准化工作。华为担任该工作组的副报告人，积极与全球各国成员协作推进区块链标准工作。另外面向物联网和智慧城市，华为携手中国联通等公司共同完成 ITU-T 国际标准《面向物联网和智慧城市的基于区块链技术的数据交换与共享》，已于 2020 年 8 月获得正式发布。

2016 年 9 月国际标准化组织（ISO）成立区块链和分布式账本技术的技术委员会 TC 307，秘书处设在澳大利亚标准协会（Standards Australia）。ISO/TC307 开展面向基础类、智能合约、安全隐私、身份认证、互操作等方向的重点标准研制工作。

中国区块链标准组织：产业活跃，国标、行标和团标快速推进

中国区块链标准组织非常活跃，2020 年中国正式成立全国区块链和分布式记账技术委员会，负责区块链和分布式账本技术领域基础标准、业务和应用标准、过程和方法标准、可信和互操作标准等，华为作为技术委员会委员之一参与区块链国标的制定。中国通信标准化协会的互联网与应用技术工作委员会(TC1)和物联网技术工作委员会(TC10)也在积极推进区块链在 ICT 领域的标准发展。同时众多区块链联盟也在围绕区块链行标和团标开展工作，标准成为区块链产业发展的重点之一。

总之，华为积极投身于各大国际和中国区块链标准组织、区块链联盟和论坛，和全球合作伙伴一起推动区块链标准化工作，共筑区块链产业及生态的快速发展。

变化 2：区块链跨链标准成为国内外区块链标准争夺的热点

目前区块链技术百花齐放，各行各业按照自身需求构建区块链应用。但各个区块链在共识机制、智能合约、通信协议等技术方面均存在差异导致无法互联互通。未来不同区块链之间的跨链互通是产业发展的必然趋势。为了解决上述问题，帮助行业达成共识实现互联互通，区块链的互操作标准显得非常重要。区块链互操作标准可以分为三类：第一，区块链之间互通的跨链标准；第二，区块链系统与应用层交互信息和接口的标准；第三，支持区块链链上链下数据安全可信交互的标准。目前各国际和中国区块链标准化组织纷纷启

动跨链标准。华为作为区块链技术深度推动者，在积极主导和参与国际和国内跨链标准，助力区块链互联互通发展。

1.1.3 全球区块链的技术发展动态

Hype Cycle for Blockchain, 2021

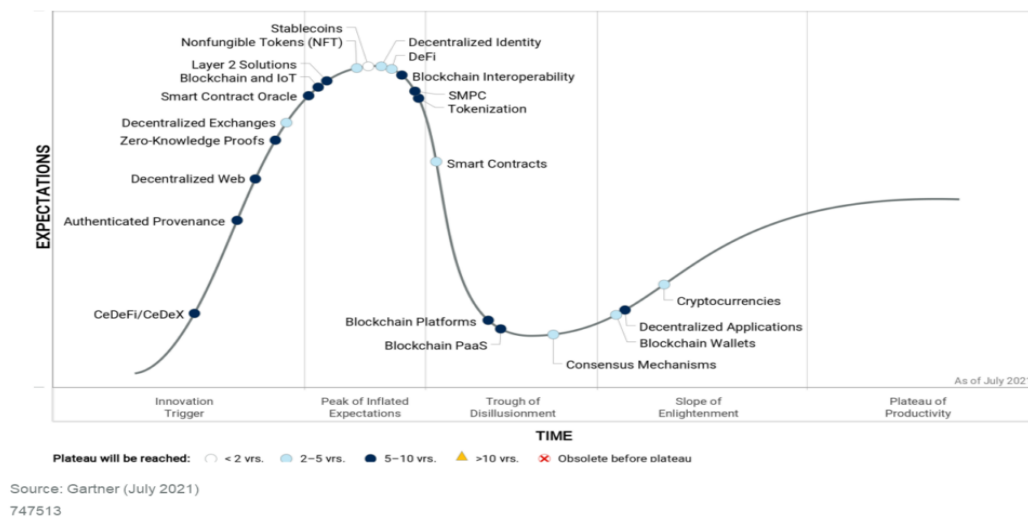


图 1-2 2021 年 Garner 区块链技术曲线

从 2021 年 Gartner 区块链技术曲线来看，区块链技术方向渐清晰并进入项目实施。跨链技术越过炒作点逐渐偏向技术务实的方向发展，而区块链平台以及区块链 PaaS 技术在逐渐进入技术成熟期。

区块链技术从 2021 年开始加速，从单一技术向多技术融合发展，通过多技术辅助实现围绕业务端到端发展。“区块链+”整体体现为区块链+IoT、区块链+5G、区块链+云计算、区块链+大数据、区块链+人工智能等，从而形成以区块链技术为核心，多技术协同的综合技术发展思路。

1.2 新形势对区块链的需求

数字经济对区块链技术发展提出四点要求。第一是技术性能提高与网络扩展的要求：节点数增加与高交易处理效率要并存，区块链隐私安全与高扩展要并行，跨链要保障一致性和原子性；第二是区块链与周边技术的交叉互通的要求：“区块链+”强调以区块链为主体与其他数字经济息息相关的技术（5G、AI、大数据等）结合，以区块链为底层核心融合各种技术形成技术融合体，构筑端到端数据要素的安全流转；第三是区块链应用与监管协同要求：区块链应用要以监管为基础而构筑的应用场景，同时监管机制成熟是推动区块链快速落地为根本。第四是区块链自身安全与过程安全要求：一方面区块链以加密算法保障基于节点的自身安全，另外一方面基于数据流转过程，需要围绕云计算+BaaS 平台+网络安全+芯片安全的一整套安全框架。

2020 年 4 月，国家发改委首次明确了“新基建”的范围，区块链技术基础设施首次被国家层面明确为新型基础设施。同年，党的十九届四中全会通过的《中共中央关于坚持和完善中国特色社会主义制度、推进国家治理体系和治理能力现代化若干重大问题的决定》，首次将数据列为与劳动、资本、土地、知识、技术、管理并列的生产要素。

区块链作为基础设施需要具备的四点特征，以构建坚实的区块链基础设施底座：

- 1) 区块链基础设施是以联盟链为发展方向，以数据要素构筑数据的可信价值传递。
- 2) 区块链作为基础设施将不在关注单一技术模式，而是依靠区块链的可信理念围绕数据业务端到端的安全为方向，形成以区块链技术为核心的多技术融合体，而高安全、高扩展、高弹性需要纳入整个区块链融合体。

- 3) 以跨链实现链链互通，解决区块链从当前“局域网”向“全局网络”发展的问题。
- 4) 区块链基础设施要赋能千行百业，依托行业特征以数据为主线构筑不同的应用，如数据共享、供应链金融、产品溯源、电子证照等细化应用，同时应用将可能从 2B、2G 向 2C 的应用进行延伸。

2. 华为区块链作为基础设施的技术与方案特点

华为区块链以融合技术为基础，不仅结合安全多方计算技术、可信执行环境技术等保障区块链技术自身应用的安全并且保障业务流在流转中的安全，而且华为区块链结合华为综合的技术特点，将软硬技术融合在区块链架构中，实现区块链+，形成从数据流的录入到数据流的分析，从数据从云平台到网络及芯片的端到端支撑，形成全民的区块链服务架构，为区块链基础设施奠定坚实的技术能力，可实现真正的链上数据确权、信息存储锚定，广泛的数据协同等以数据安全流转为目标的应用实施，形态成为数字基建的新基石。

2.1 华为区块链发展思路及方向

2.1.1 华为区块链发展史介绍

华为区块链经历了三个发展阶段，第一个阶段（2015 年-2018 年）为探索期：华为从 2015 年启动对区块链技术的研究，并纳入华为 2012 实验室进行技术孵化，以研究技术的可行性并作为重要创新技术发展，同期华为是 Hyperledger 重要成员，不仅在 Hyperledger Fabric 和 Sawtooth Lake 项目贡献大量代码，担任国内仅有的项目 Maintainer 职位，而且也为 Hyperledger 社区贡献了区块链性能测评工具 Caliper 项

目；第二个阶段（2018 年-2020 年）为成型期：华为于 2018 年 2 月推出华为云区块链服务 BCS（Blockchain Service）进行公测，在公测期间有约 1000 多家企业试用。

2018 年 10 月 BCS 正式商用，内核是基于 Hyperledger Fabric 的华为增强版本，为用户提供一站式高性能区块链服务。在这一阶段，BCS 服务了七大领域（政务服务、医疗健康、工业、金融、文娱版权、能源、物流）涉及 400 多个 PoC 及正式商业应用，加速区块链产业应用发展；第三个阶段（2020 年-至今）为成长期：数字经济发展对区块链技术提出了更高的要求，特别是跨链、分布式身份、隐私计算，共识算法，智能合约、链上链下协同、区块链网络等都需要进一步完善，且秉承国家对区块链要求强化核心技术发展的要求，2020 年华为 BCS 集合前期经验，发布华为自研的区块链内核引擎——华为链，突出技术自强自立，安全隐私、高并发等能力，既能满足千级节点的可靠组网诉求，同时可满足在大规模节点环境下保持单链 10 万+TPS 的高性能处理能力，华为希望将技术做深做透，让业务围绕区块链能够构筑端到端的安全保障。

2.1.2 华为区块链目标：深耕联盟链核心技术，愿做数字经济的筑基者

1. 华为区块链的“双核”发展战略

华为云区块链服务（BCS）是基于华为分布式并行计算、存储、网络、安全、加密、容器等核心技术领域多年积累推出的企业级区块链云服务产品，为开发者提供可信、便捷、高性能的区块链生态环境和生态配套服务，支持开发者业务拓展及运营的区块链开放平台。

根据国际和国内对区块链核心能力的多样化诉求，华为云区块链服务提供“双核”区块链引擎供用户选择，其中包括华为自研区块链内核引擎（华为链）和 Hyperledger

Fabric 华为增强版。1) 华为链由华为区块链研发团队研发，华为链在架构设计上参考了业界成熟的区块链技术框架但突出华为区块链平台的自立自强，结合华为在硬件、网络、安全等方面的优势，在性能和规模上提高了数十倍，安全方面提供了基于 TEE 的支持，及纯软件层次的安全隐私保护，同时在架构上增强传统区块链的 BaaS 层，强化区块链的服务层的能力，让区块链在技术保障的同时提升易用性。主要定位于国内对安全、高性能的行业应用的诉求，例如国内的政务服务、金融等具备高并发和高安全要求的行业。2)

Hyperledger Fabric 华为增强版是基于开源社区 Hyperledger 的区块链 Fabric 基础的重构与增强，优化并重构了共识算法、对安全、加密、可靠性等一些商用特性，即实现代码的自主升级又兼容 Hyperledger 的社区版本能力，其应用主要针对海外科技及与海外 fabric 平台的友好对接应用场景。

华为云区块链服务（BCS）全面支持“双核”引擎，纵向结合了华为在云计算、硬件、网络、安全、软件等各方面的优势，是优势资源调度的“双核”区块链操作系统，是软硬一体的融合式区块链服务体系架构，在发展中技术相互兼容，特性拉齐，并行发展。同时基于“双核”引擎提供 BaaS 和 APaaS 层的服务能力，帮助企业快速、高效的搭建商业级区块链服务，并实现业务和应用的一站式集成。

2. 华为区块链做好基础设施的“筑基者”角色

随着数字经济的发展，传统的区块链很难保障业务流特别是数据流的端到端安全，因此我们不能再拘泥于单一技术，我们需要面向时代发展的需求，重新审视区块链。由此，我们从以下三个方面对 BCS 服务进行了重构，以期为数经济发展提供可支持大规模应用、可信安全的区块链基础设施。

第一、华为区块链与 IoT、5G、AI、大数据等技术协同，实现数据可信上链、可信传递、可信分析的端到端服务。华为区块链与 IOT 技术结合解决上链数据可信，与 5G 结合解决区块链边缘节点的组网要求，与 AI、大数据结合解决群体智能的可信分析。

第二、华为以纵向做深，围绕云、网、端、边、芯构筑纵向安全框架。华为区块链服务平台负责区块链记账、共识等安全保障，区块链网络提供可信的网络传输，提升区块链数据在传递中的低时延、高带宽以及网络内生安全的防护。区块链边缘节点提升区块链处理及时处理能力，而芯片提供 TEE 环境实现合约、共识等算法与 TEE 结合，构筑可信的安全环境。

第三、华为区块链提供 APaaS 服务能力，具备数字身份管理服务、数据共享服务以及隐私保护服务。华为区块链的 APaaS 不仅可与区块链应用层友好对接，同时联动华为区块链内核，可更好的助力用户便捷的部署新业务。

2.2 华为区块链的技术特点

2.2.1 华为区块链的技术架构

目前 BaaS (Blockchain as a Service 区块链即服务) 最流行的模式是区块链云服务，狭义上也把 BaaS 称作区块链云服务。例如，IaaS 是把计算资源作为服务，PaaS 是把软件研发的平台作为服务，SaaS 是把软件作为一种服务。BaaS 作为一种云服务，是区块链设施的云端租用平台，其多租户特性让计算资源、平台资源、软件资源得到了最大程度的共享。BaaS 提供节点租用、链租用以及工具租用的能力，其中工具包括开发工具、部署工具、监控工具等，并通过大容量的资源池，保障租户的业务规模可灵活弹性伸缩，

租用设施可共享和独享，安全可靠运行，此外还提供必要的技术支持服务。BaaS 的具体能力包括区块链节点及整链搭建的能力、区块链应用开发的能力、区块应用部署的能力、区块链运行监控和管理的能力。华为区块链服务提供的整体架构是基于 BaaS 体系的增强所提炼的新型架构模式。

华为区块链服务整体架构（如下图 2-1 所示）分为四层：基础设施层、基础 BaaS 层、区块链基础服务层、行业应用场景层。



图 2-1 华为区块链 BaaS 架构图

2. 基础设施层

通过云环境，IOT 设备或者专有设备在专有或者公有网络上提供必要的计算资源、存储资源、网络资源等基础设施支撑。为系统提供扩展存储、高速网络、安全芯片及按需弹性伸缩和故障自动恢复的节点等资源。

3. 基础 BaaS 层

基础 BaaS 层是在基础区块链底座和基础跨链底座的基础上封装了中间件服务，为上层应用提供必要的底层服务及扩展的能力，使能千行百业。基础区块链底座是基于自研的华为链和增强版 Hyperledger Fabric 通过高安全的密码学技术保证传输和访问安全，支持在海量节点组网的网络环境下，使用华为自研高性能共识算法，确保链上数据的一致性、安全性及区块链应用的稳定运行。基础跨链底座通过华为自研跨链流程，通过中继链及可信硬件提供一整套可信安全的跨链体系架构，保证不同链数据交互的一致性、可追溯及可审计等。

中间件层分为管理组件和扩展组件，管理组件包括用于平台管理、节点管理、联盟管理、运营管理的管理组件、用于为用户操作提供便捷如区块链浏览器、区块链应用商店等功能服务；扩展组件包括用于实现链上数据隐私安全的隐私保护组件、用于节点身份验证的身份认证组件、适配不同监管要求的安全组件、联盟链成员内部自治的联盟链治理组件、为数据提供更高安全级别的可信执行环境适配模块等。不同中间件组件的作用都是为了提高区块链的易用性，扩展区块链的使用边界，从而简化区块链的开发、部署及运维，降低区块链应用门槛，提高区块链的面向复杂场景的可用性。

4. 区块链基础服务层

区块链基础服务发挥区块链融合云计算的技术优势，为区块链开发提供便捷、高性能的区块链系统和基础设施服务。便于政府、企业和开发人员高效的使用区块链，快速构建和维护区块链应用；同时支持对不同的区块链平台进行统一资源管理、统一身份认证、统一运营监管、统一生态协同。平台提供可视化部署能力，实现一键式区

区块链网络的自动化创建，异构区块链的一键接入，解决上链难的问题，降低区块链使用门槛。其中基础服务层，包含以下三层：

1) 管理服务 and 标准接口

统一标准纳管接口定义了不同底层区块链需要遵循的接口规范，包括统一安全、统一运营、统一资源管理、统一跨链和统一监管五大类；底层区块链区块链的统一管理基于统一纳管的区块链资源提供的管理功能；基于这一套标准为客户屏蔽中间件及底层链相关管理接口，更好的支撑管理服务。用户可以在不深入了解区块链的前提下使用上述服务，以此保证业务场景在安全、稳定和高效的环境下持续运行，并极大程度降低政府及企业的运维成本，达到降本增效的效果。

2) 统一区块链管理层

服务管理层包括了必要的平台功能管理及运营管理。为链上节点提供如区块链浏览器、区块链应用商店等功能服务，使操作用户能够更方便、快捷地使用系统平台，同时提供多种不同底层链的运维服务，从而简化区块链的开发、部署及运维，降低区块链应用门槛，提高应用灵活性。

区块链服务层提供智能合约商店和应用商店。商店可用于发布、管理多种业务的智能合约应用，包括存证合约、上链合约和交易合约等，减少对已有成熟模式的重复造轮子问题，丰富行业领域应用生态

3) APaaS 层

基于目前区块链难使用的问题，华为定义了自己的 APaaS 层服务，打造了区块链的 serverless 服务，给不同 ISV 或者用户提供访问接口，支持数据直接上链，屏蔽了中间件和链的感知。使企业和研发人员无需考虑区块链底层技术，专心搭建区块链上层应用。通常情况下，开发人员在创建链和智能合约时，面对的是一行行计算机代码。而如果采用 APaaS 层服务，这些代码被事先写好，模块化成常用的功能接口，研发人员只需通过 API 接口，连接这些功能，降低中小企业使用区块链的门槛。在区块链投入运营后，利用服务提供的监控功能，通过系统采集到的日志，可以在任意时间即时查看到维护当中的区块链的运行情况，同时，在运行指标接近阈值时，服务可以在第一时间发出告警通知，减轻区块链维护人员压力。

5. 行业应用场景层

行业应用场景层是各类管理和服务主体根据业务协同需求构建的链上应用，华为的应用场景主要应用于政务、金融、医疗、司法等各个领域。

2.2.2 华为区块链关键的核心技术

华为区块链秉承做好筑基者推动区块链基础设施服务数字经济发展。区块链要服务数字经济需要坚实的技术能力及未来的技术演进能力，在华为区块链核心技术重点体现如下关键能力：高性能、高扩展性、高安全性、高可靠性、高效的互联互通性及软硬协同性。

华为区块链的核心技术分为三大类：

第一类：性能类技术——突出区块链业务处理的高并发性及组大网的能力

1. 高性能：满足单链 10 万 TPS 吞吐能力，在动态分片下可实现 TPS 近线性增长

金融、政务、智慧城市、互联网等行业对区块链高并发的需求，对区块链性能提出了高标准要求。区块链并发性能与共识算法优化紧密相关。目前业界多以实用拜占庭容错 PBFT 共识为主要方式，虽然可满足基本应用，但是这种方法性能提升难度大（当前华为最高调优可达 1.3 万左右的 TPS 能力），且存在通信复杂度过高的问题。RAFT 共识效率虽高但无法容忍拜占庭错误。华为区块链将 RAFT 共识与可信执行环境相结合，利用可信执行环境防止了拜占庭错误的发生，有效的提升了 RAFT 共识的安全性。同时华为区块链对交易内容进行压缩瘦身，可以达到单链 10 万 TPS 的吞吐量。此外，采用华为自研动态分片方案，可实现区块链 TPS 近线性增长。

2. 高可扩展性：当前已实现千级节点组网能力，未来面向万级节点组网

传统区块链的联盟链，由于点对点网络针对共识和区块复制的消息冗余度较高，区块链系统的运行效率随节点数增长会呈现快速下降的趋势。同时传统区块链的应用场景，依托不同的链构筑不同的独立应用，形成割据的“局域网”，导致应用用不起来，性能上不去，数据量不足等问题。伴随着区块链应用会越来越需要跨区域、跨城市、跨国家的组网要求，节点数量会因应用延展而剧增，单条链上需要支持大规模节点并能够正常运行区块链服务。

当一个区块链集群节点数拓展到百级时，因为单个节点需要维护百级的 TCP 连接，造成大量内存消耗，集群收敛速度缓慢而不稳定，尤其在容器部署场景更加明

显。为了实现千级和万级节点扩展的目标，首先要解决 TCP 连接数过大，和由于随机通信造成的流量过高的问题。

华为区块链对性能和可扩展性进行平衡，采用树形结构的方式支持大规模网络扩展。通过对网络进行分层分区治理，通过算法优化，大幅降低网络内部的消息冗余度，从而使得区块链系统的运行效率不会因网络的扩容而出现明显下降。当前华为区块链可支持千级节点的组网能力，通过支持多个分片的并行处理，2021 年年底可实现单链万级节点的网络规模能力，同时通过采用轻节点可有效降低资源开销，实现低开销下的区块链组大型网络的组网需求。

3. 高效存储能力：基于分布式存储的高效混合存储引擎提升存储效率

传统的区块链在处理海量数据方面存在欠缺，因此高效的混合存储引擎是大规模数据区块链应用的关键技术之一。针对大规模数据的应用场景以及不同的数据类型，华为区块链设计了不同的存储引擎，以支持基于区块链的分布式存储技术与链上链下数据协同、海量数据的存储与处理，实现大数据的链上存储以及不同类型数据的链上链下分离，使得系统读写性能不受影响，实现高效的存储与分发。

区块链的每一个节点都存储有链上数据的完整副本，并且每个交易数据上链后会附带相应证书、数字签名等数据导致容量膨胀好几倍，全网节点规模的扩大将对区块链的存储能力和响应度提出很大挑战。华为区块链通过数据压缩和交易瘦身特性，将单区块链节点的数据膨胀比降低到 1:2 以下，从整体上极大地降低了存储成本。

4. 低开发学习成本：基于关系数据库的区块链存储技术

在传统业务中，企业往往基于关系型数据库的结构化数据模型构建和表达业务，而目前区块链的存储数据库仅支持键值对存储，当业务系统需要对接区块链系统时会带来极高的成本。新型区块链存储技术基于关系型数据库，支持各类复杂业务的结构化建模、高性能的数据写入、复杂快速的数据查询，对开发人员友好，可大幅解决企业用链难的问题，帮助企业快速上链，高效复用已有代码，降低开发成本。

5. 高效合约执行能力：高效智能合约体系配合高安全的合约保障助力应用可信执行

针对不同场景和参与方，一套高效的智能合约体系将能够推动区块链落地。智能合约体系需要支持多种智能合约引擎和多种主流智能合约编程语言，提供完善的合约生命周期管理，支持用户通过业务流管理等可视化工具自动生成智能合约代码，降低研发复杂性和成本，支持灰度升级，做到编程友好、合约安全、执行高效、版本升级平滑过渡，以支持各种分布式应用，适应复杂多变的业务场景。让客户简单使用区块链系统，更专注于上层应用的创新和开发。同时针对客户的合约也提供静态扫描和形式化验证能力，提供军事级合约安全能力。

第二类：安全性技术——突出区块链业务端到端的安全保障能力，提升数据要素的可信

1. 高安全性：华为区块链自底向上构建了全方位的安全保障体系

区块链系统是一种信息系统，因此传统信息系统所面临的安全威胁对区块链是同样存在的，所以传统的安全防护机制，工程手段都不容忽视。华为区块链基于华为云，自底向上构建了全方位的安全保障体系。华为云已通过多项国际权威安全认证，为华为区块链提供了安全合规的基础底座。在此基础上，华为区块链在关键领域如共识算

法、同态加密、零知识证明、电信级云安全，高速网络连接、海量存储等方面具有自主知识产权的专利和技术积累。此外，华为区块链还充分结合可信执行环境，利用硬件的安全能力，将共识算法核心逻辑、智能合约执行引擎、跨链中继器等关键组件纳入可信执行环境内部实现，使得区块链的安全级别得到进一步提升。

在密码算法方面，华为区块链支持 RSA/ECDSA/AES 等通用加密算法，同时还支持国密 SM2/3/4 算法，提供多种加密算法供用户选择，满足安全合规要求。

在网络通信层面，区块链的服务端节点之间，以及区块链的客户端和服务端之间均采用 TLS 通信协议，在交易消息中还会携带交易发起方的数字签名，以保证数据的完整性。

在智能合约层面，华为区块链提供智能合约安全检查工具，防止恶意的企图通过智能合约漏洞入侵用户数据的行为，同时提供安全容器，持续监控容器的运行状态，一旦发现漏洞，将进行有效的隔离，对容器的访问权限进行严格控制，从而保证合约安全运行。同时，华为还在进行智能合约语言方面的研究，期望在未来，从合约语言的层面提供安全简洁的编程接口。

华为区块链可提供基于密码学的隐私保护方案，又能提供结合可信执行环境的软硬协同隐私保护方案供用户使用。华为区块链在交易解决方案中：（1）提供同态加密库，对用户的交易数据用其公钥进行加密保护，交易的时候都是密文运算，最终账本中加密保存，即使节点被攻破，获取到账本记录也无法解密；（2）提供范围证明校验，背书节点能够对密文进行背书，无需解密就能校验交易的正确性，从而识别出恶意交易风险，保证

了智能合约的正确执行；（3）提供基于可信执行环境的隐私保护方案，通过隐私保护数据访问接口实现的智能合约，可以在 TEE 内进行数据处理，从而保护隐私数据不被泄露。

2. 高可靠性：通过计算、存储、网络解决区块链节点可靠性问题

华为区块链分别从计算、存储和网络三个角度考虑区块链节点的可靠性问题。

计算：基于华为云容器引擎构建，华为云容器引擎使用业界主流的 Docker 和 Kubernetes 开源技术，集群控制面支持 3 Master HA 高可用，当其中某个或者两个控制节点故障时，集群依然可用，保障业务高可用。集群内节点和工作负载支持跨可用区

(AZ) 部署，构建多活业务架构，保证业务系统在主机故障、机房中断、自然灾害等情况下可持续运行，获得生产环境的高稳定性，实现业务系统零中断。此外，还可通过 web 界面轻松实现集群节点和工作负载的扩容和缩容，自由组合策略以应对多变的突发浪涌。基于华为云容器引擎的能力，当区块链节点出现故障时，系统会对故障节点进行自动恢复，从而保障区块链应用的可靠性。

存储：华为区块链服务将租户的账本存储在弹性文件存储系统（Scalable File Service, SFS）中，弹性文件存储系统采用三副本备份，提供按需扩展的高性能文件存储（NAS），可为云上多个弹性云服务器（Elastic Cloud Server, ECS），容器（CCE&CCI）、裸金属服务器（BMS）提供共享访问，数据持久性高达 99.99995%。通过 VBS（Volume BackupService）实现云硬盘的备份与恢复，且支持通过弹性文件系统备份创建新的弹性文件系统。在确保弹性扩展的基础上通过一系列的安全措施保障账本的安全。

网络：华为区块链采用了网络分层分级算法，实现节点数的大规模扩容。在节点分层的同时，通过算法保证每个节点仍然能与多个周边节点进行互联，使得区块链网络的健壮性不下降。

第三类：互通性技术——突出区块链及周边技术的互通协同能力

1. 链上链下的技术协同：实现链下数据的可信获取

当前各个领域对于区块链应用的探索正在如火如荼的展开，但是进展缓慢的原因是当前的区块链网络相对于现实世界，是一个信息孤岛，即区块链无法获取现实世界的数据。链下的数据显然无法完成整个业务闭环。当前绝大部分业务都还是运行在传统的中心化系统中，其业务数据无法获得区块链系统的信任，也就很难与区块链系统结合起来。因此区块链如何可信的获取链下数据也是当前的重点发展方向。

要实现链下链上数据协同，就要解决链下数据的信任问题，主要有两个方面。一是数据源的可信问题，如果源头都不可信，那一切就无从谈起。另一个就是可信上链的问题，即使从可信数据源获取到有效的数据，也要保证数据的确为请求的数据，且传输过程没有被篡改。数据源一般跟实际业务相关，数据源可信，需要开发者保证，即确保合约访问可信的 Web 系统、数据库等。

当前链下数据获取的探索大致分为两个方向。一个是去中心化的链下数据获取方案，多个节点组成一个新的链下数据获取网络，也称之为预言机网络，预言机网络同样是一个区块链服务。当链上节点需要获取链下数据时，发起一笔跨链交易。预言机收到交易请求后，执行数据获取命令，执行结果达成共识后才能生效。链上节点再通过访问预言机的链

数据，获取可信链下数据。去中心化链下数据获取网络的优点很明显，其彻底贯彻区块链的去中心化特性，满足可信需求。但其缺点也非常明显，获取链下数据的代价较大，流程复杂，延时高。且只能支持 Web 等这种公开数据，场景非常受限。

另外一种则是中心化链下数据获取方案，链下数据服务提供商通过公司信誉，可信硬件等手段保证上链数据的可信问题。去中心化链下数据方案虽然完美的契合了区块链，但其缺点导致其无法很好满足工业区块链的场景。中心化链下数据方案可以高效、低延时的响应数据获取请求，同时可以适配 Web、SQL、Driver 等各种数据引擎，满足不同场景下丰富的需求。其缺点即为大部分中心化网络的通病，容易产生单点故障。

华为云区块链服务采用中心化链下数据获取的方案，华为作为利益不相关的第三方，致力于提供安全可靠的链下数据获取服务。区块链网络需要链下数据获取服务时，只需在链下数据获取服务进行申请，华为云区块链服务分发相应密钥，完成服务注册。区块链网络需要获取链下数据时，只需将自己的请求使用密钥进行加密，发送给链下数据获取服务。身份验证完成后，将请求命令及结果等信息再加密返回给区块链网络，区块链网络完成身份认证后，即可完成数据上链。

为满足日益丰富的业务需求，华为云区块链服务下数据获取服务的可以满足 Web、SQL、可信硬件等类型的获取请求。同时数据获取驱动采用插件化设计，可以随时满足新的需求。华为链下数据获取服务还将采用分布式架构，提供容灾能力，解决中心化链下数据获取服务的单点故障问题，提供稳定、可靠、可信的链下数据获取系统。

2. 区块链与 IOT 协同能力：借助 IOT 加密等方式解决可信上链的问题

在物联网行业链条中，往往末端的商业场景运营商对区块链可能发挥的作用有敏锐的嗅觉，但其传统的物联网终端供应商，很可能不具备开发区块链相关功能的能力，无法提供满足其需求的设备。主流的区块链服务供应商，往往对碎片化的物联网行业了解不深，试图将其区块链服务落地在碎片化的物联网设备中也会遇到很多困难。在这样的背景下，具备连接区块链能力的通信模组，即区块链模组应运而生。

华为云和摩联科技共同推出了基于区块链模组的解决方案，区块链模组并非全新的模组品类。如下图 2-2 所示，区块链模组本质上就是在现有开放的协议栈层次体系上，又叠加了一层区块链客户端协议。应用可以向这层区块链客户端协议，请求区块链交易、智能合约调用等区块链服务。区块链客户端协议再进一步结合密钥生命周期管理、设备 Attestation 等，就构成了基于模组的 BoAT 区块链应用框架（BoAT blockchain application framework），或者称为 BoAT 设备钱包（BoAT Device Wallet）。

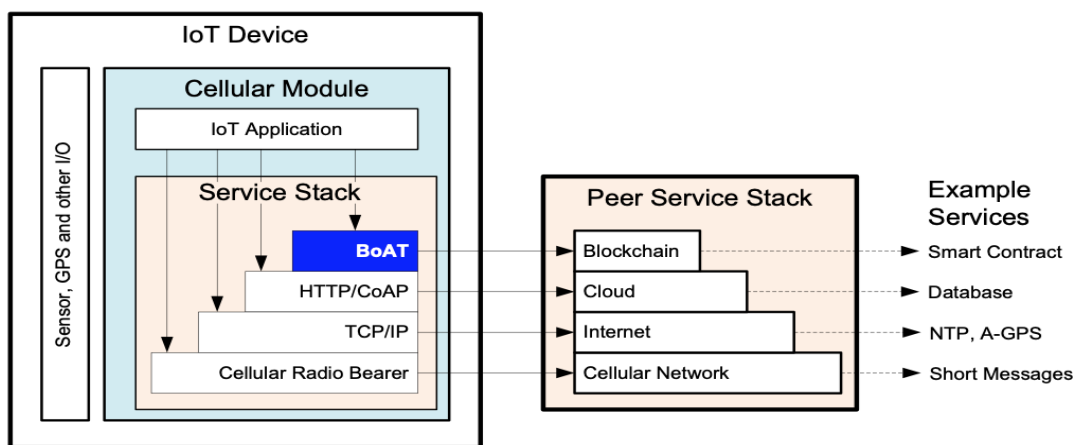


图 2-2. 区块链模组支持下的物联网业务栈

绝大多数物联网终端受成本、功耗等因素限制，其能力通常是较为受限的。能力受限的物联网终端，通常不同步账本、不参与共识，而是作为区块链客户端，在物联网终端上链过程中，直接或间接向区块链节点发起智能合约调用交易。

能力受限物联网终端的上链过程，一般具有如下图 2-3 所示的典型参考架构。

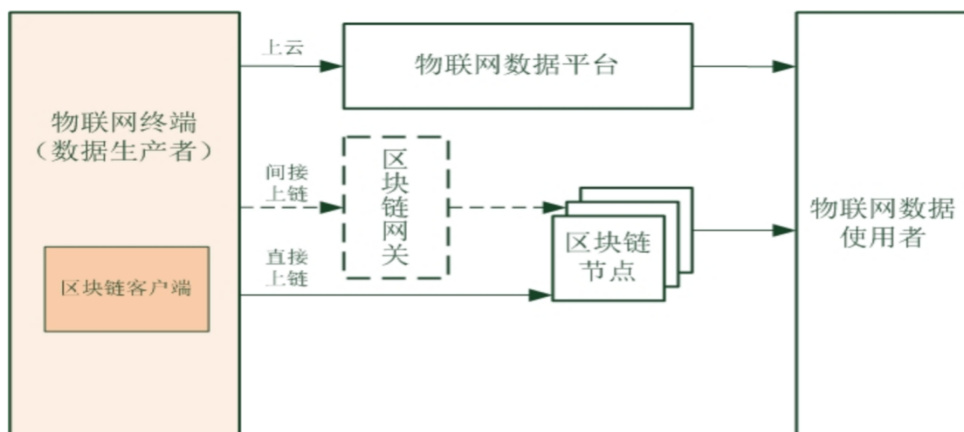


图 2-3. 物联网终端上链参考模型

在能力受限物联网终端上链参考模型中，物联网终端作为数据生产者，在原有将数据上云的基础上，将相关信息直接或经由区块链网关间接上链。而物联网数据使用者，则通过访问区块链获得可信的上链数据，并结合云上数据，实现数据的可信使用。

为了让物联网数据具有适当可信度，终端设计应结合对成本、数据价值等方面的要求，综合考虑抗远程攻击、抗本地攻击等方面的安全目标。能力受限物联网终端数据上链，需要终端具有一机一密的公私密钥对，并作为客户端访问链上的智能合约服务，并且通常（但不限于）以物联网数据作为访问智能合约服务时的参数。对区块链上智能合约而言，物联网终端通过数据上链的过程，扮演了区块链预言机的角色。上链的数据既可在合约中存储下来用于后续可信验真，也可以作为合约逻辑输入条件或运算的输入参数等。根

据不同的智能合约需求，物联网数据既可以将数据本身上链，也可以将数据的指纹上链。若将数据本身上链，应特别注意链上数据访问权限以及个人信息处理符合国家有关法律法规。若将数据上云，而将数据指纹（一般为数据的杂凑值）上链用于事后验证云上数据的完整性，那么上链信息和上云信息中应包含能够关联两者的标识，令上链的数据指纹，与上云的数据能够一一对应。若能力受限物联网终端因某种原因，无法直接访问区块链节点的服务（例如，蜂窝物联网终端的流量为定向流量且不能连接区块链节点；物联网终端不支持区块链节点远程过程调用所使用的通信协议等），可将上链数据发送至区块链网关，再由区块链网关上链。上链信息中，必须包含终端签名相关的信息，以确保网关无法伪造或篡改来自终端的数据。

3. 区块链网络的互联加速：P2P 无法保障业务链接的安全性，需要区块链网络提升 互联的带宽、降低互联的时延、增强网络的安全

当前区块链的一个重要瓶颈就是性能（可扩展性）问题，其性能一般以 TPS（Transactions Per Second）来描述，TPS 是一个有成熟定义的计算机术语，代表了系统每秒钟能够处理的业务

数量是衡量一个系统吞吐量的核心指标。简单地说，TPS 越高，这个系统的事务处理能力越强，越不容易造成网络拥堵，在高并发的业务领域和商业级应用场景中有很大的优势。TPS 越低，意味着系统每秒能够处理的事务数量越低，如果是在一个支付系统中，交易速度会越慢，对应的交易成本也会越高。由于 TPS 是一个量化指标，所以其计算公式是确定的，即：
$$\text{TPS} = \text{系统并发数} / \text{平均响应时间}$$

区块链网络即 Block Chain Network(BCN)，简单将这些技术划分为通信协议技术、P2P 网络技术、网络安全技术等，华为着眼从底层网络技术优化区块链整体性能。华为依托 BBR(Bottleneck Bandwidth and RTT)技术提升 TCP 的吞吐量，降低网络传输时延；依托网络的防拥塞丢包技术（iLossless）解决网络或设备自身拥塞导致丢包，可快速缓解网络拥塞，消除网络丢包，可有效解决当前区块链网络上对时延和性能的要求；依托确定性 SLA、组播数据分发和数据压缩等技术，从各个维度优化区块链网络的性能，如确定性 SLA 是优化 P2P 网络的时延和抖动，同时也有有效避免端到端的网络连接的拥塞，从而保证区块链的 P2P 网络的高质量的 SLA 并获得更高的性能。而组播分发和数据压缩可以一定程度减轻链路上带宽压力，充分利用网络的能力，并最高效的利用网络带宽。

区块链网络的架构如下图 2-4 所示：

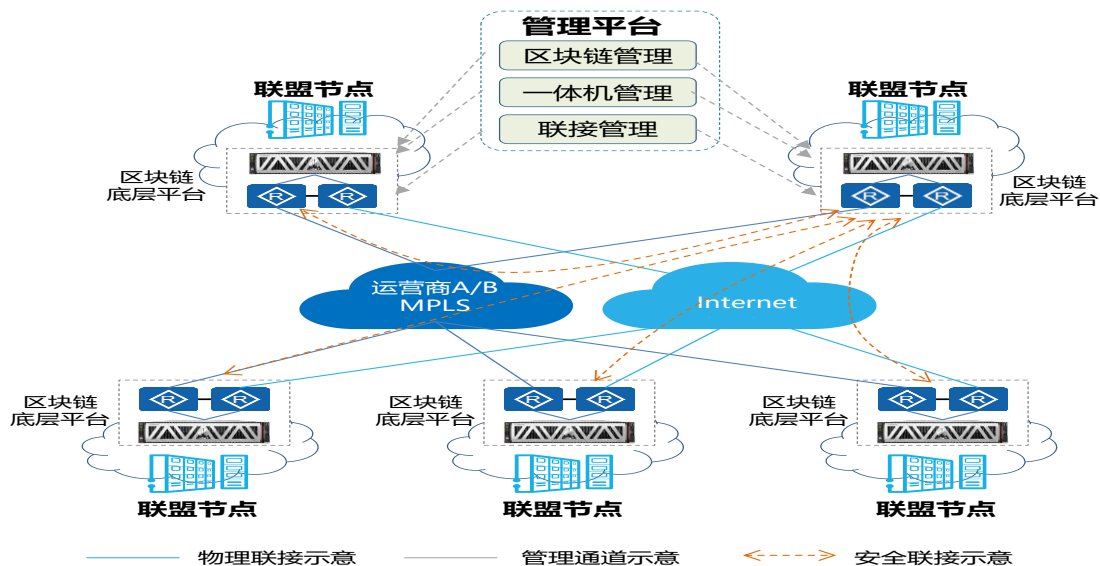


图 2-4 华为区块链网络组网图

华为区块链网络提供区块链节点部署，多站点部署，可支持 FullMesh 互联，总分互联，以及互联网互联等，可按需进行任意安全互联。各节点间通过安全联接隧道两两互

联；各联盟节点统一管理，包括联接管理、一体机管理（节点物理机）和区块链软件管理；业务自动化，包括远程或新节点的快速启动，联接自动打通，自动接受管理平台纳管；业务联接优化，包括 FEC 防丢包、TCP 优化等，安全提升包括 ACL 过滤、防火墙和 IPS 等；解决方案架构包含管理平台、联盟节点和联接网络三部分，首先，管理平台包含了区块链软件、一体机和联接等三部分，联接管理平台主要是针对每个节点的网络节点（按出口路由、安全设备和交换机等），以及节点间网络连接（可以是专线、VPN 专线或 Internet 专线）的管理，物理设备和联接链路的管理。联盟节点，即部署在联盟链成员单位的区块链节点，当然该节点可以根据功能定位的不同，有不同的节点配置，即节点形态。联接网络相对容易理解，节点内网络设备组网和安全策略，节点间的物理链路及其之间的安全 VPN 建立。

2.3 华为区块链 APaaS 服务栈

为了让区块链应用、区块链 SaaS 更快更好落地，让行业开发者更聚焦于行业业务，华为推出了一揽子开箱即用的区块链 APaaS 服务，让使用者不用关心资源、运维，只需要结合业务逻辑来调用 APaaS 的接口来实现应用功能。以下介绍几个典型的华为区块链 APaaS 服务。

2.3.1 可信分布式数字身份服务(TDIS)

华为区块链可信分布式身份服务(Trust Decentralized Identity Service, TDIS)是一种基于区块链的分布式数字身份及可验证凭证的注册、签发、管理平台。符合 W3C 标准规范。为个人和企业用户提供统一的、可自解释的、移植性强的分布式身份标识，同时支持

多场景的可验证凭证管理，细粒度的凭证签发和验证，有效解决跨部门、跨企业、跨地域的身份认证难和隐私泄露等问题。

TDIS 包含 6 个主要功能。其一、身份管理。提供分布式身份标识的统一管理能力。包括用户身份的创建、更新、验证、恢复、服务发布等基础能力，同时提供 Resolver，支持链外解析能力；其二、认证管理。提供功能强大的统一认证体系。基于分布式身份标识，可完成可验证凭证的申请、签发、授权、组合出示、验证等能力。同时，凭证模板管理能力方便用户构建标准化的业务凭证体系；其三、隐私保护。通过密码学算法保护凭证申请、签发、出示等全流程的数据安全。基于分布式身份提供可信的数据交换和共享；其四、密钥托管服务。提供密钥托管服务，减少用户维护分布式身份所需公私钥的复杂性，降低密钥丢失带来的安全风险。支持通过 RESTful API 调用管理分布式身份；其五、链上链下认证。支持通过链上和链下两种方式完成凭证的申请和签发。链上模式，通过智能合约可自动化完成凭证使用的全流程管理。链外模式，可以更好与已有业务系统结合，支持应用快速上链；其六、分布式身份插件。支持以插件的形式在已有区块链服务上安装部署分布式身份，用户可通过证书、私钥以及 API 灵活方便地使用分布式身份和可验证凭证的管理能力，快速构建应用。

TDIS 具备以下三点优势：第一、具备全球兼容的分布式身份系统。遵循 W3C 的 Decentralized Identifiers(DIDs)v1.0 和 Verifiable Credentials(VC)v1.0 标准规范，系统扩展性强，支持身份和可验证凭证的全流程链上管理能力；第二、具备强数据隐私保护能力。可验证凭证支持基于属性级别的细粒度出示，凭证使用者可根据隐私保护需要，任意组合出示凭证中的属性给验证者完成验证，最大程度保护用户隐私，同时解除了已签发

凭证对应用业务场景的限制，凭证申请和签发的相关材料全链路加密存储，使数据可用不可见；第三、拥有丰富的扩展组件。提供凭证模板管理、可信数据交换协议、积分支付、链下凭证签发等扩展功能组件，帮助用户基于分布式身份快速构建应用；其四、具备简单低门槛接入便于应用部署。支持密钥托管和插件部署两种方式，满足用户的不同需求。密钥托管模式下，通过简单易用的 RESTful 接口轻量接入使用，无须购买和管理区块链资源，插件部署模式下，通过证书、密钥使用分布式身份。

2.3.2 可信数据交换与计算服务(TC3)

可信数据交换与计算服务(Trusted Data Exchange & Computing Service, TC3)基于区块链共享账本，为链上应用提供支持多参与方之间的可信数据资产交换和可信联合分析计算能力。通过数字水印技术嵌入数据使用者的信息，提供数据交换全生命周期的追踪溯源能力，便于追责定界。建立可信沙箱计算容器环境，实现数据提供方、使用方、执行方的三权分置能力，做到数据“可用不可见，可见不可得”和“用后即焚”的功能。

TC3 具备的功能有四点。其一、数据可信交换。基于区块链，实现用户认证数据的发布、申请、授权、评价等能力，同时数据交换支持开启积分支付、评价等扩展功能；其二、身份管理。统一的身份管理体系，提供身份的创建、更新等功能，用户可以基于分布式身份完成数据交换和计算，保护用户隐私；其三、数字水印。针对不同数据类型提供添加水印的能力，结合区块链技术实现数据交换全流程的保护；其四、可信计算。为每个参与方提供基于 Spark 的可信沙箱计算环境，通过区块链注册和管理计算节点，实现算法的

发布、申请、授权、执行、结果上传等。全流程通过密码学算法进行隐私保护。算法支持类型包括大数据分析计算、机器学习分析、SQL 数据查询等。

TC3 具备四点优势。第一、操作可审计。数据交换和计算的申请、授权、评价等操作行为完整保存上链，全流程自动、透明、可监督，支持事中校验、事后审计，保障多方权益；第二、数据确权追溯定责。数据目录、摘要、所有者等信息上链，快速完成确权共识，共享数据中加入使用方信息水印并更新上链，在发生数据泄露时，追踪源头定界定责；第三、数据安全隐患保护。数据交换和实时计算中，数据内容与计算结果均进行加密保护，链上授权链下解密使用，支持国密算法；第四、可信安全计算。建立可信沙箱计算容器环境与区块链系统的对接，完成基于可信硬件的多方数据安全计算和联合分析，支持大数据计算、机器学习、SQL 查询等。

2.3.3 可信跨链数据链接服务(TCDAS)

在区块链场景中面临最大挑战便是多链形成的信息孤岛。随着区块链系统和应用的成长和发展，链间的通道成为瓶颈，它阻碍了区块链间的协同操作，很大程度限制数据和信息流转的效率和范围。解决多链交互的诉求愈发明显，跨链技术制约区块链发展的关键技术点。

主流跨链技术包括：（1）公证人技术：通过第三方“连接器”来实现不同链上的信息、资产转移；（2）侧链/中继：侧链使用新的链来锚定主链上的账本信息，从而实现基本的信息验证、资产转移、互操作性等能力；（3）哈希锁定：链间设定相互操作的触发

器，先披露明文的随机数的 hash 值，通过锁定一段时间后发布 hash 原值来兑换支付的机制。

华为根据该领域的特点以及针对落地过程中存在的权限控制、身份管理、安全隐私的问题，提出了可信跨链的解决方案和服务能力。

1. 开放的身份体系

身份体系是通讯的基础，目前很多跨链解决方案中并未重视区块链身份体系的搭建，区块链跨链标识往往只能在局部跨链使用，跨链作为面向万链互联的基础设施，区块链身份体系将会是重要基础。现在开放的互联网安全通讯里，已有一份健全且久经考验的体系：PKI 基础设施。开放的跨链互联网络有着与现有互联网一致的需求，即开放、安全通讯、分布式自治。而不同的点是该区块链证书的对象是一条链及链上对象，对于链的身份，这里涉及到如何开放地定义链的“唯一标识”，对于链上的对象，包括账号以及合约等，要考虑如何出域对外可验证。业务引入了与 PKI 体系类似，但更具轻量级、分布式自治与扩展性的“分布式身份”体系，让业务在由区块链组成的价值互联网里进行安全跨链，做到“有根可寻”、“安全可控”。

2. 完善的权限管理

跨链过程中仅在所有者授权情况下才能进行，通过身份体系制定被授权的区块链及区块链合约，进行数据调用或合约消息通讯。保护数据安全同时，实现数据使用的可追溯。

经过数据授权，业务合约发出跨链数据访问请求，通过跨链寻址，将跨链网络上对应区块链上的数据安全可靠的返回给请求者。

用户可以授权其他区块链的指定智能合约，推送跨链合约消息，经过跨链寻址，实现合约的远程调用，完成业务场景中的复杂互操作。

3. 更强的安全跨链能力

异构区块链账本上的可信数据的数据格式、验证逻辑、验证信任根都是独立的，其规格可以通过区块链自身协议定义清楚，任意客户端包括另外一条链上的单位，原理上都可以直接认证。但在实际跨链中更多存在中继者等角色做了一层“桥接”，桥接过程中完成原数据的安全认证、数据格式转化、数据重新声明等动作，本质上这些行为是一种“证明转化”：在不改变原有数据语义的前提下，进行数据格式转化、数据证明的转化、信任根的转化，以便于验证者安全简便地解析和认证跨链信息。华为可信跨链服务把以上过程梳理成协议，即“证明转化协议”，使其可以清晰地描述流转跨链消息时数据格式验证规格以及数据语义的信任根，最大保障了跨链协议的安全性。

3. 华为区块链的典型应用实践

华为区块链自 2018 年在华为云上线商用 3 年以来，合作伙伴、各地政府和企业基于华为云区块链服务构建了数百个应用落地场景，使能千行百业，包括如下图 3-1 所示场景：

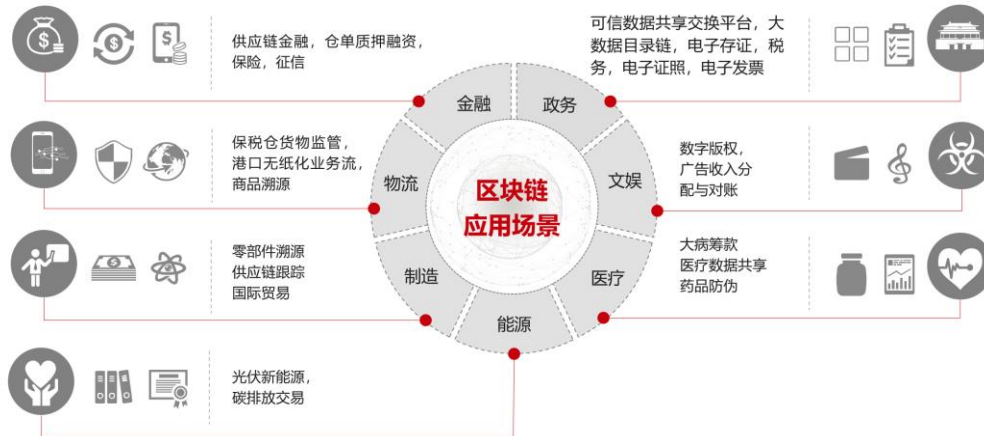
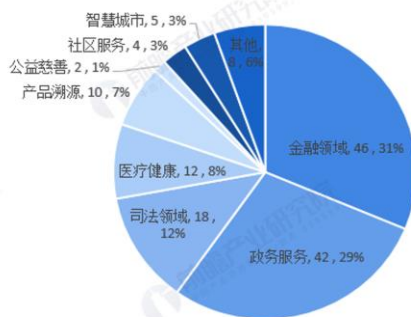


图 3-1 华为区块链应用的行业领域

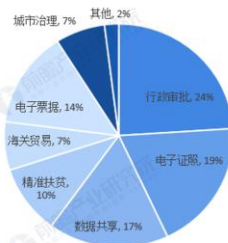
根据市场调查和华为区块链实践，区块链现阶段应用热点主要分布在政务与金融两个板块。区块链在金融、政府服务、司法等领域的应用发展尤为活跃，占总体落地项目的 31%、29%和 12%。同时，区块链在医疗健康、产品溯源领域的应用也在加快推进。

图1-2020年区块链场景分布统计



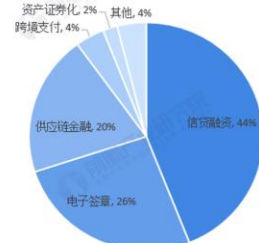
资料来源：赛迪、区块链研究院 前瞻产业研究院整理

图2-2020年政务区块链场景统计



资料来源：赛迪、区块链研究院 前瞻产业研究院整理

图3-2020年金融区块链场景统计



资料来源：赛迪、区块链研究院 前瞻产业研究院整理

图 3-2 区块链场景分布统计（source：赛迪等机构）

在华为部署案例中选取政务、金融和医疗健康三个区块链活跃领域典型落地案例进行详细阐述。

3.1 城市大数据可信共享枢纽—目录区块链

3.1.1 背景：基于区块链实现政务数据的统一调度、管理和控制

“数字城市”、“智慧城市”已经成为中国城市发展的大趋势。近年来，以 5G、人工智能、云计算为代表的新兴数字技术的广泛应用，以及“新基建”的推进，让数字城市、智慧城市的构建明显提速。数字城市强调，看得见、有得用，注重基础、以数据主导。而智慧城市注重应用，根本原则是“以人为本”，以“为民、便民、惠民”为导向，让大数据用起来、用得广、用得好。

2018 年某市大数据行动计划实施以来，华为区块链协助某市通过一年时间，利用区块链将全市 53 个部门的职责、目录以及数据联结在一起，解决了数据缺位、越位的问题。同时依托“目录区块链”将部门间的共享关系和流程上链锁定，建构起数据共享的新规则，解决了数据流转随意、业务协同无序等问题。所有的数据共享、业务协同行为在“链”上共建共管，无数据的职责会被调整，未上链的系统将被关停，建立起部门业务、数据、履职的全新“闭环”。针对各部门数据共享难、协同散、应用弱，企业、百姓办事困难等难题，全面提升政务服务水平，支撑营商环境进一步优化。

“目录区块链”系统：是指利用区块链的公开、分权、不可篡改等特性，建立以“职责”为根的三级目录体系。其核心是建立了基于职责的政务数据共享和考核的新模式，实现政务数据的统一调度、管理和控制。

3.1.2 痛点：解决数据共享难问题

某市 2006 年建成了早期市区两级共享交换平台，实现与国家共享交换平台的对接，及接入了 16 个区和 69 个市级部门。但存在数据未落地，只是交换通道作用，数据交换与目录存在脱节问题，数据共享和开放不全面等问题。

国家2007年发布标准：GBT 21063.x-2007 政务信息资源目录体系



图 3-3 某市目录系统存在的问题

这导致政府部门共享信息过程复杂。根据市经信局大数据建设处相关负责人举例说，市水务局想要市规划自然资源委“建设用地规划许可证”和“建设工程规划许可证”两项数据，用于支撑其供排水接入营商环境的政策措施落地。市规划自然委会担心：怎么给数据才安全？数据给出去到底用在哪了？水务局也会担心：沟通协调需要多长时间？获取的数据质量可不可靠？这些顾虑在现有的共享体系中导致委办局之间数据共享需要数周或者数月的时间，社会机构甚至没有途径获取政务数据。

3.1.3 方案：依靠区块链实现数据可用不可见，可见不可得

某市目录区块链利用区块链的分布式存储、不可篡改、共识及合约机制等特点，将政府各部门的职责目录和关键数据目录“上链”锁定，实现数据与职责的强关联、数据变化的实时探知，及数据访问的全程留痕，保证各部门目录的可见、可用、可考核，从根本上解决目录不全、目录与数据“两张皮”、目录变更和数据共享授权随意、数据更新不及时等传统“老大难”问题。

目录区块链中承载了全市大数据的确权和分权管控机制。作为某市大数据整体工作的“定海神针”，其核心作用体现在：数据在政府内部和政企之间流转的所有动作，已发生的都由“链”来记录、在发生的都由“链”来管控、将发生的都由“链”来驱动。“链”上所有逻辑的背后，是从管理角度建立了一套基于职责的考核体系。

目录区块链体系由市区两级构成，其中市级目录区块链分为“步道-链道-数道”三层架构。其中：步道是目录链管理应用主要解决决策问题，实现管理、共享和考核，核心在于链上和链下的关系；链道主要解决管控问题，通过智能合约实现逻辑管控和统一调度；数道主要解决执行问题，提供明文和密文的数据传输和处理能力。如下图 3-4 所示：

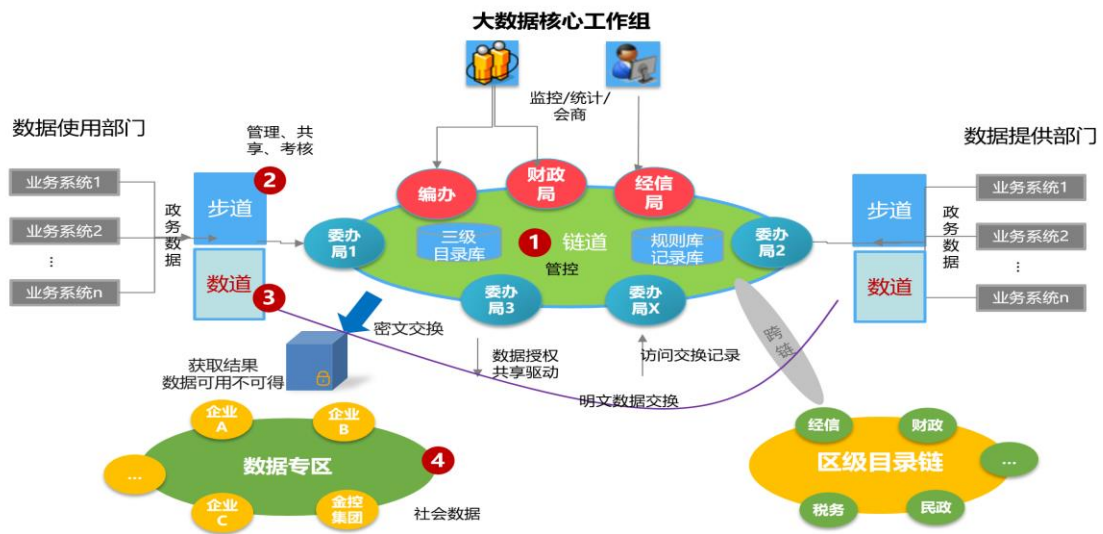


图 3-4 华为云某市目录区块链解决方案

- 1) 链道：由市经济和信息化局、市委编办和市财政局牵头政府各相关部门组成区块链联盟链，并逐条梳理建立“职责目录”，对应形成全市基于三级目录体系的“数据目录”一本大台账，利用区块链的分布式存储、不可篡改、合约机制等特点，建立起某市“目录区块链”，将各部门目录“上链”锁定，实现了数据变化的实时探知、数据访问的全程留痕、数据共享的有序关联，通过分布式技术从根本上解决了分布式数据共享难题。

三级目录链体系：在国家编目指南基础上，某市大数据目录体系细分为“职责目录-数据目录-库表目录”三级目录结构。其中：职责目录：主要用于数据确权（依据三定职责，依法采集、依法授权管理和履职产生的数据资源），由各部门编制，市委编办、市经济和信息化局联合审定。具体包括：部门名称、处室名称、职责、数据资源名称、核心数据项、所属信息系统名称；数据目录：主要用于数据共享（职责目录中数据资源和数据项的具体描述），由各部门编制，市经济和信息化局审定。具体包

括：数据资源名称、数据资源摘要、数据起始日期、数据更新周期、数据格式、数据项、数据类型及长度、是否主键、是否非空、共享属性、开放属性、数据量等；库表目录：主要用于目录与数据关联（数据目录中数据项的具体存储描述），由各部门编制确定。三级目录结构的核心是“对应”，即明确“职责-数据-系统”之间的关系。本质上是从数据角度做了两件事：一是技术上定到“系统”，二是管理上找到“处长”。在此基础上，以职责为“根”，重点进行“剪枝”（系统整合）、“壮干”（数据共享）。没有数据的职责取消，没有职责的系统关停。

- 2) 步道：主要解决管理、共享和考核工作包括以下几个方面工作：目录链上链，政府部门“上链”内容为职责目录、数据目录和信息系统基本信息，社会机构“上链”内容为数据目录；市大数据平台汇聚数据统一按照“人-企-物”的基础框架进行“原子化治理”和“标签化管理”，并依托目录区块链提供“画像式服务”；链上审核，按照《某市目录链管理规则（试行）》和《某市目录区块链审核细则（试行）》， “链”上内容的变更由市委编办、市经济和信息化局、市财政局 分别从编制统筹、资金统筹、数据统筹的角度进行审核；可以完成发起数据共享申请发起和申请审批；并对年度、月度数据上链和共享项目进行考核和排名促进共享，实现闭环。
- 3) 数道：是大数据共享执行的关键部分，通过明文和密文两种方式满足政务、社会数据可信共享和交换。

- a) 明文方式：链道通过驱动数据交换合约根据授权和共享方式调用华为云 ROMA 分布式实时数据交换平台以 API 接口调用或者数据库迁移的方式完成数据共享，

实现数据目录、共享条目、权限管理、共享日志全部通过区块链技术上链，让交换机制可追溯，可信赖；同时 ROMA 平台还可实时反馈数据状态。实现数据跨组织高速共享交换、数据变化实时探知、数据访问全程留痕、数据共享有序关联。

- b) 密文方式：某市利用目录区块链结合沙箱、多方安全计算等技术开展“数据专区”探索，目的就是针对金融、医疗、交通、教育等数据热点需求领域，推进政府数据的社会化利用。以“金融数据专区”为例，某市大数据平台开辟“金融数据专区”，并将其作为某市政务数据在金融领域社会化利用的统一接口，授权金控集团代为运营，通过目录区块链将政、企两端的数据统一管控、授权共享，打通企业应用和政府管理之间的数据壁垒，基于沙箱和多方安全计算实现数据可用不可得，在确保安全的前提下充分释放数据“红利”。

3.1.4 成效：提升智慧政务效率，增强民生服务体验感

通过目录区块链，实现数据申请、授权、确认、共享的全流程，取代以往复杂的沟通、协调模式；2019 年 10 月，首个线上数据共享流程依托“目录区块链”开启，市水务局对市规划自然资源委以上两项数据的共享，申请、授权、确认、共享、使用等各环节均在“目录区块链”管控下自动执行，10 分钟内全部完成。

基于目录链区块链关键应用助力营商环境改善，有“区块链”加持的大数据，能给市民带来明显的“获得感”。

目前，某市不动产登记“一个环节、一天办结”。去年，这个业务涉及交易、缴税等 4 个环节，时间需要 5 天，还需要提供户口簿、结婚证等一大堆纸质材料。现在，只要登录“某市不动产登记领域网上服务平台”或者到不动产登记大厅就可以体验方便快捷的新流程，且只有一个环节、一次性即可办结。

这背后是目录区块链调度下的全市各部门数据有序运转。通过“链”上实时调用公安、民政等多个部门的户籍人口、社会组织等标准数据接口，实现了减材料、减流程、减时间。

据今年世行报告，某市建筑许可办理时间压缩了 32%，环节压缩了 18%，排名大幅提升。自 2017 年 12 月起，某市就通过大数据平台共享了建设工程规划核验、建设规划许可证信息等 20 类数据，对压缩建筑许可审批时间提供了支撑。如今在目录区块链的支撑下，共享完成了闭环的最后一步。

3.2 医疗健康——基于区块链的医联体

3.2.1 背景：医疗机构与健康保险机构数据拉通是关键

从 2013 年 9 月份以来，国家先后出台了《国务院关于促进健康服务业发展的若干意见》和《国务院关于加快发展现代保险服务业的若干意见》，《关于加快发展商业健康保险的若干意见》，从国家层面连续出台鼓励和支持商业保险发展的政策文件，提出**将商业健康保险建成医疗保障体系的重要支柱**，在构筑民生健康保障网、完善多层次社会保障体系、推进健康服务业整体发展中要发挥重要作用，显示了国家对商业健康保险的高度重视。

3.2.2 痛点：数据不安全、信息孤岛等制约医疗健康及医保体系

当前医疗保障体系和保险体系还存在以下的问题。

- 数据不安全：医疗健康数据大多是存在数据中心，如果数据中心发生自然灾害、黑客入侵等，那么患者的电子病历就有可能彻底丢失
- 信息孤岛：医疗机构之间没有合理的互信机制和良好的分享机制，容易形成“信息孤岛”，不利于数据的完整性和全面性。信息的可靠性，以及在共享中信息的随意修改都成为面临的主要问题。
- 重复医疗：由于各个医院和机构之间信息不互通，患者去一家医院就会在该医院建立一份电子病历，使患者重复做各种检查，耽误时间、金钱以及医疗资源
- 无获得感：医疗资料产生与患者却存放在医院系统中，患者对自己的数据不了解，也无法掌控，患者的就诊与健康管理受有限资料的限制

3.2.3 方案：构筑可信区块链医疗平台，打通医疗数据提升幸福感

医联体是由医疗、保险、金融等商业机构构建的可信区块链医疗平台，提供个人的实名认证、政务数据的安全共享、在线安全支付、个人征信数据的采集等功能，作为医疗行业实现先诊疗后付费、商保直赔等普惠服务的基础支撑。通过可信连通、安全的入口支撑、政府大数据公共服务支撑下实现医疗行业医疗关系的改善，提升市民就医体验，提高医院工作和管理效率。基于区块链技术的医联体平台组网结构如下图 3-5 所示：

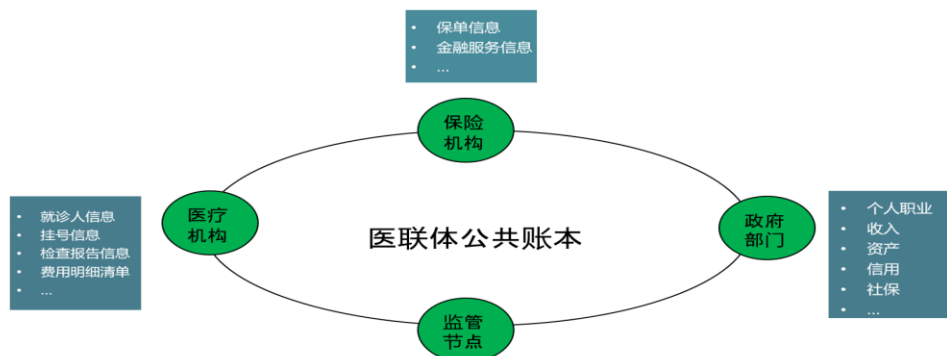


图 3-5 基于区块链技术的医联体平台组网结构

医联体平台由可信区块链网络、应用门户以及政务公共服务三大体系形成安全可信的行业应用支撑平台。

可信区块链网络：利用区块链技术构建普惠医疗网络，实现政府与、医疗、金融、保险等机构之间数据的共享与协作，政务公共服务提供个人职业、收入、资产、信用等数据；医疗机构提供就诊人信息、挂号信息、检查报告信息、费用明细清单等数据；金融服务机构借助政务公开数据利用智能合约的支撑，实现对个人就医的创新普惠金融服务，并通过区块链网络公开业务办理关键节点的流转状态。

医联体以应用门户为依托，实现多重实名认证、安全私钥保障、多种支付方式以及各行业功能入口等功能。整合政务各类业务数据、电子证照、社保信息以及信用采集评估等公共服务资源供各医疗机构、商业机构进行调用。区块链医联体网络将承担政府部门与机构间所有数据交互的安全、高效、便利的通道。

医联体网络连接各级政府部门、医疗、金融、保险等机构，金融和保险机构借助平台提供的多重市民认证、政务公开数据、政务公共服务为依托，为市民提供普惠医疗服务，内容包括先诊疗后付费、健康险、医疗分期等各种商业服务，通过医联体平台的可信连

接，医疗、金融、保险机构可以与相关政务部门实现业务联动与高效协作，这些服务汇聚到医联体 APP，提高市民获取医疗服务的便捷性与丰富性，缓解市民就医负担。主要场景介绍如下：

“先诊疗后付费”：该制度是卫生部在 2013 年起全面推行的一项医疗保险制度，由医院先垫付医疗费，病人看完病只需交纳自己那部分费用，其余费用由医保部门直接支付给医院。这项利民惠民的制度，由于户籍制度限制和医保和财政体系不互通等问题，存在结算难、病人身份难确定、诚信制度落后等问题，导致一部分无能力归还高额医疗费用者，欠款风险高，医院切身利益无法保障，在推行时却存在一定的困难。

基于区块链技术的先诊疗后付费系统，整合政府部门、医疗机构、金融机构数据，用户可通过医联体 APP 线上申请先诊疗后付款，银行调用智能合约根据政府的个人征信数据和就诊信息给出医疗金融产品，便捷高效的为市民提供就医救助，减轻市民就医负担。

“商业医保直赔”：因医院与各保险机构信息系统相互隔绝，商业医保报销流程非常复杂。商业医保理赔需要被保险人提交资料、等待保险公司受理、审核、放款，周期较长。报销时除需提供基本身份资料，还要出具医院盖章的病历、费用清单、化验单、收据等诸多资料。

基于区块链的商业医保直赔系统，整合政府部门、医疗机构、保险机构等数据，所有参与方共享一个包含公民全量信息、医院就诊数据、保险服务数据的加密账本，投保商业医保的患者省去复印病历、跑保险公司、等待结账等麻烦的手续，出院后在医联体 APP 上申请，用户在 APP 上申请保险理赔，保险机构自动调用智能合约，根据医院上传的就诊信

息和个人缴纳的保险信息给出理赔结果，实时办理商保结算业务，快速获得理赔，如下图

3-6 所示：

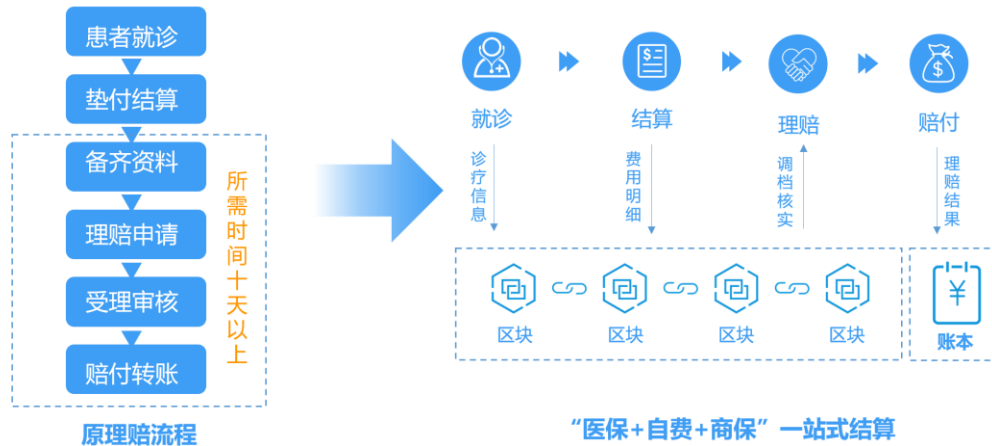


图 3-6 区块链在医疗保险中的应用模式

3.2.4 成效：完善医疗救助体系，增强全民健康指数

通过医联体平台可以完善医疗救助的事中即时结算和事后委托结算机制，提升医疗救助结算管理水平；支持社会力量提供多层次多样化医疗服务，推动商业保险机构遵循依法、稳健、安全原则，以战略合作等方式整合医疗服务产业链，探索健康管理组织等新型健康服务提供形式。

医联体平台将发挥以下作用和价值：

1. 医疗数据共享：实现政务数据的对外开放以及医疗数据的实时共享，并且数据真实可信，可追溯。减少保险公司核验成本

2. 多方业务协同：搭建社保、医院、保险机构间的数据通道，打破医疗行业数据壁垒，推进医疗医保数据协同，支撑商保直赔、快赔、先诊疗后付款等业务的多方协同在线办理，客户可在线上直接申请，理赔流程更便捷
3. 隐私安全保护：个人授权查询医疗数据，智能合约控制查询权限，保证隐私数据安全。
4. 形成开放生态：通过区块链技术建立的可信网络，后期可快速、低成本的接入银行等金融机构，提供更丰富的创新金融医疗服务。

3.3 智慧金融——区块链的供应链金融

3.3.1 背景：供应链环节多，环节出差将导致重大损失

某能源集团其供应链环节多，如招标采购、金融保险、物流运输等，且每一个环节出差错都会造成重大损失，因此其将整个能源供应链搬到“云”上，构建集中采购平台、电商销售平台、智慧物流平台、金融科技平台及大数据云平台等体系，实现商流、物流、资金流及信息流的“四流合一”，打造能源物资智慧供应链集成服务平台。

该集团结合华为云区块链服务，打造行业区块链供应链金融服务平台，基于区块链技术建立起来的供应链信用机制则被称之为“能信”。在此基础上，双方还联合开发了一种分层加密的功能，使供应链信用变得更透明，业务也更简单。“能信”不仅提升了供应链信用度，还能为“链”上企业省钱。“如一个发电厂在进口煤炭业务中使用了‘能信’，

获得供应商让利，一吨煤就少花了两块钱，供应商融资成本可降低 4%左右，还能提前近一个月回笼资金，综合物流降本增效空间约 10%。

3.3.2 痛点：信息不通，合同造假等导致集中模式下确权难

传统供应链金融面临的问题主要是四点：

- 1) 造假风险——仓单、票据等造假；
- 2) 企业信息孤岛问题，企业间系统不互通，贸易信息主要靠纸质单据，四流难合一，增加银行对企业信息获取的成本且让风控难度提升，从而增加了企业融合的难度；
- 3) 核心企业的信用不能跨级穿透：核心企业信用智能传递至一级企业，其他供应商无法利用核心企业信息用金融供应链融资；
- 4) 违约风险高——单凭合同约定，融资企业的资金使用及还款情况不可控，资金被挪用，融资企业违约拖欠或恶意违约等问题。

3.3.3 方案：借助区块链实现信用穿透助力供应链企业融资

区块链+供应链金融构建供应链金融的业务创新，如下图 3-7 所示



图 3-7 区块链+供应链金融的系统架构

区块链+供应链金融对比传统业务模式，优势主要体现在为：

- 1) 实现四流合一，区块链难篡改使数据可信度高，降低企业融资及银行风控难度；
- 2) 风控数据获取、合同签订、票据流转等业务执行线上化，周期短、效率高；
- 3) 凭证可多级拆分融资，解决非一级供应商融资难、资金短缺问题；
- 4) 智能合约固化资金清算路径，极大减少故意拖欠资金等违约行为的发生。

1. 项目需求

该集团的能信体现核心企业的商业信用，是核心企业基于应付账款向其供应商在线开立的应收账款债权凭证。持有人可以将能信拆分流转、在线融资或持有至到期收款。能信到期，开立能信的核心企业会将能信结算资金支付至能信所有最终持有企业的支付账户。

基于区块链技术搭建的华能供应链金融区块链服务平台，节点包括运营方、核心企业、供应商和资方四方。使用区块链技术可在各参与方之间共享安全可信的能信数据，并实现能信数据的不可篡改和可追踪溯源，支撑应用层实现能信的开立、转让、融资和兑付等业务场景。

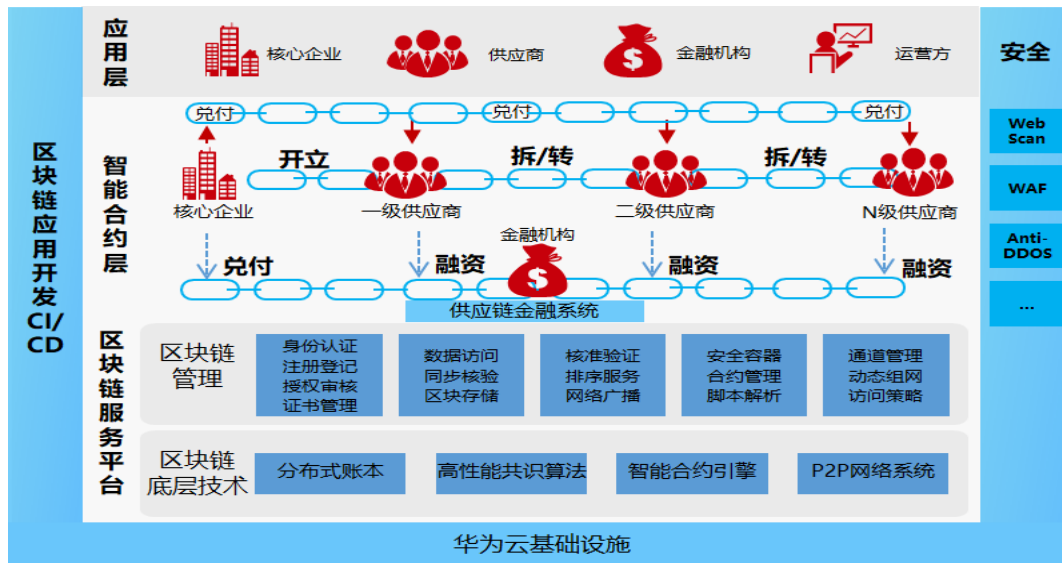


图 3-8 供应链金融的整体方案框架

2. 项目部署方式

平台运营方建立联盟链，联盟链参与方包括运营方、核心企业、供应商和资方。由核心企业基于应付账款申请能信开立，运营方经过审批和复核之后，能信开立成功，全部转让给一级供应商，供应商可以发起转让、融资业务申请，能信到期兑付。

所有参与方全部参与背书共识记账，共同见证，杜绝篡改和伪造。能信的业务流程与归属清晰，从能信开立、转让、融资到兑付均可完整追溯。供应商可以随时根据其持有的能信发起融资申请，资方可以依据共享的能信数据进行快速审批放款，有效提升供应链金融的整体效率。

根据需求描述进行分析，华能供应链金融区块链服务平台包含以下信息上链需求：存证交易信息、多签地址信息、能信开立信息、能信票据信息、能信转让信息、能信兑付信息，这六种信息上链。

3. 项目关注问题

在区块链供应链金融的业务部署中需要关注的问题，主要有三点：

- 1) 与核心企业关联企业上链的沟通问题，相关企业要作为联盟节点接入区块链，其需要承载一定的产品和运营成本；
- 2) 区块链供应链金融建立的是以核心企业为依托的信用穿透。核心企业开具可信的债权凭证（如案例中展示的能信，一种体现核心企业的商业信用，是核心企业基于应付账款向其供应商在线开立的应收账款债权凭证），而供应商不能自己申请开立债券凭证，只能对接收到的债权凭证进行拆分、转让和融资。因此方案设计中要保障核心企业的债权凭证的开具上链成为供应链金融的关键；
- 3) 产品开发及部署后，面临的专利及知识产权的归属问题。客户有时会表示希望拥有相应开发的知识产权的问题，因此，可考虑助力客户对相关专利的申请，也可考虑在相关技术上实现知识专利共享的方式，以解决客户对专利的要求。

3.3.4 成效：降低供应链金融风控，提升集团供应链企业的稳健性

基于华为云区块链服务（Blockchain Service）解决了供应链金融最重要的环节风控，而风控里最重要的环节是“控货”（监控货物的运输过程），基于区块链可以有效解决‘货找车，货找船’的问题”；其次，随着平台稳定运行，有一定的数据量的基础后，就可以用大数据的手段进行分析和预测，目前平台上有数万辆货车，每个司机每天通常会完成多个运单，通过运单数据可以分析出相关信息：运输线路情况和车况等；如基于数据分析

可以将一定期限内无事故完成一定数量运单的司机定义为优质用户，可以在运费结算政策上进行倾斜。通过这些供应链的数据分析，可以形成一个司机或一支车队的用户画像，区分出其服务信用的等级，为平台上的企业及金融用户进行金融服务提供可信的参考数据。

华为与该集团在区块链技术应用上，结合物联网手段，实现供应链金融服务。使用区块链之后，数据就不再像传统数据库那样可以篡改。电力行业的供应链金融服务引入区块链技术后，就会形成四方机构：电厂(核心企业)、供应商、平台方和资金方。这四方在区块链上都有各自的节点，进行分布式记帐，大家都同时拥有帐务信息，保证了不可篡改性。在此基础上，电厂的信用可以通过平台向供应商传递，在四方机构共同认可业务的基础上，作为资金方的银行也不需要单独去授信某一个企业，只要供应商提供平台上核心企业开具的票据，银行便可以直接兑付。

4. 华为区块链的发展展望

从 2009 年比特币诞生至今，历经 10 余年，区块链技术已经有了长足的进步。从最早仅支持虚拟货币交易的公有链，逐步发展出适用于企业、行业的私有链、联盟链，在性能、安全、隐私保护方面都取得了很大的突破。区块链以其去（弱）中心化、难以篡改、便于追溯的特征，逐步在金融、政务、民生、制造、文化等领域得到了初步应用，成为打造可信新技术基础设施的重要组成部分。

2019 年 10 月，业界著名咨询公司 Gartner 发布了《2020 年 10 大战略技术趋势的预测》（Gartner Top 10 Strategic Technology Trends for 2020）。该项报告研究的是在未来 5 年内迅速增长、高度波动、预计达到临界点的企业技术趋势，意味着

这些技术趋势在未来 5 年内不仅更加确定能够落地，而且还会引发商业或商业场景趋势。在这份报告中，提出了实用区块链的理念，报告指出虽然由于一系列技术问题（包括可伸缩性和互操作性）的存在，使得区块链对于企业部署仍然不成熟，但在当前的区块链实验和小型项目中，采用了一种实用的方法，通过使分类账独立于单个应用程序和参与者，并在分布式网络中复制分类账，以创建重要事件的权威记录，从而只实现完整的区块链中的部分元素。拥有访问权限的每个人看到的信息都是相同的，并且通过拥有一个共享区块链简化了集成。而共识则通过更传统的私有模型来进行处理。Gartner 认为，在未来，随着 AI 和 IoT 等互补技术开始与区块链整合，真正的区块链或“完整的区块链”将有潜力改变行业，最终改变经济。

4.1 华为对区块链的产业展望

趋势 1：整体发展环境向好，产业扶持力度加大

2019 年 10 月 24 日，习近平总书记在中央政治局第十八次集体学习时强调，把区块链作为核心技术自主创新的重要突破口，加快推动区块链技术和产业创新发展，体现了国家对区块链核心技术的重视。

2020 年 4 月，区块链技术被纳入新技术基础设施。这也是区块链技术基础设施首次被国家层面明确为新型基础设施。

据不完全统计，国内已有 22 个省市发布了区块链相关的产业政策，国内经济发展趋势和政策扶持导向给区块链发展带来机遇，政务、金融、贸易、溯源、存证、医疗、工业互联网等领域将成为区块链应用的突破口和主战场。

趋势 2：平台化服务化

2018 年以来，区块链即服务（BaaS）成为全球云平台厂商的标配，苹果、亚马逊、思科、华为、阿里、腾讯等都相继推出自己的 BaaS 平台，基于云平台的 BaaS 平台成为入门门槛，如下图 4-1 所示：

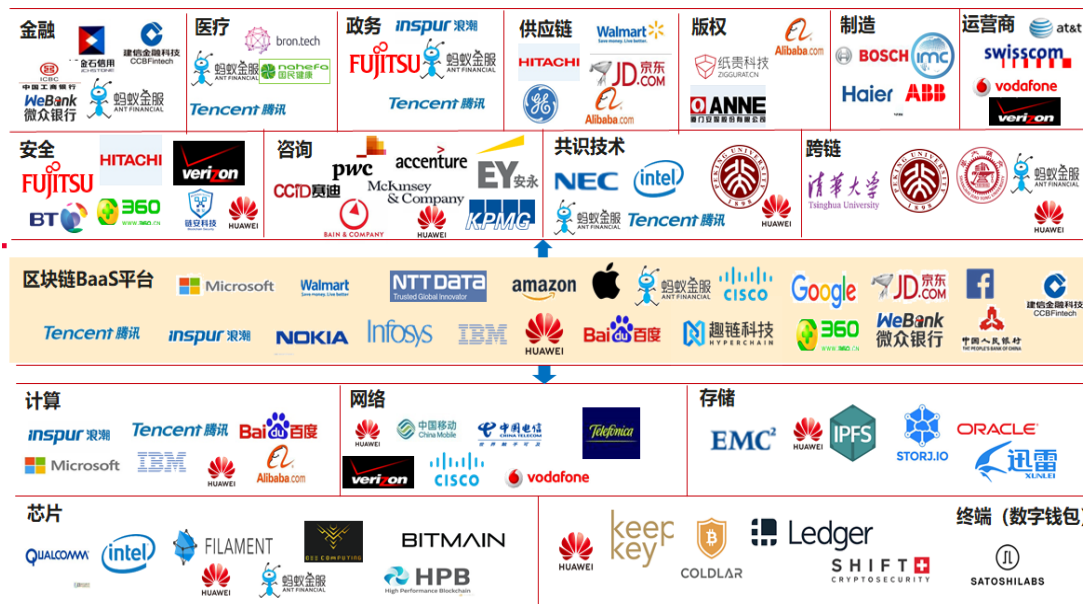


图 4-1 区块链产业布局地图

区块链服务平台化配合软件与硬件能力构筑面向行业应用成为根本。华为区块链依托自身技术优势实现软硬协同，打造坚实的区块链底座。

趋势 3：应用多向落地，行业渗透程度攀升

随着区块链解决方案的丰富和示范应用的落地成熟，区块链的行业渗透率逐步提升。在金融应用方面，以供应链金融、贸易金融领域为主，形成了较为成熟的商业模式。在政务、民生方面，以数据开放共享，一网通办等示范应用为主，利用区块链技

术优势，促进行业数字化改造升级，推动行业全方位探索实践，促进区块链技术在更多行业应用落地。

4.2 华为对区块链的技术展望

4.2.1 区块链自身技术的发展趋势

趋势 1：自研底层区块链引擎比例增加

随着区块链在各行业应用中的不断发展，基于开源架构的区块链平台逐渐遇到性能、规模、安全性的瓶颈，限制了其在更广泛的业务场景中的落地。为了满足更高的性能要求，覆盖更多的业务场景，各大区块链供应商纷纷搭建自研区块链引擎，华为从 2020 年投入自研区块链研发，2021 年 9 月华为全连接大会上正式发布商用。

截至 2020 年 10 月 30 日，国家互联网信息办公室已发布 4 批境内区块链信息服务备案清单，累计 965 个区块链信息服务名称及备案编号，华为区块链 BCS 成为首批注册企业之一。各科技公司对区块链技术和商业应用的持续探索，也加速了区块链的技术发展和业务落地，区块链应用目前也在金融、政务等各领域应用中遍地开花。

趋势 2：性能持续突破天花板

对于单个联盟区块链网络来说，通常会采用拜占庭容错的共识算法，但随着共识节点数量的增多，节点之间需要交换的信息显著增加，使得系统和网络通信量增大，造成联盟链整体性能下降，因此，通常单个联盟链网络的规模都不大。

业界在联盟链的性能提升方面进行了多个方向的研究，包括创新的交易机制、分片并行扩展、高性能的共识算法、高效的智能合约引擎，以及软硬件的协同优化。

在面对业务并发诉求越来越大的压力下，单个区块链的性能在通过分片、多链等方式可以在部分场景中大幅提高交易的并发能力。在不同的业务中，需要考虑选用适合于业务的分片策略，减少跨片的交易数量，避免跨片交易带来的性能损失。

在联盟链高吞吐量的情况下，存储面临的压力也会更加凸显。假设每笔交易实际承载的内容为 200B，加上交易的签名、数字证书等其他数据，按 20000 TPS 的交易平均吞吐量计算，每秒将产生 20MB 以上的数据量，一天就会累积达到 1.7TB，一年将达到 630TB。如此庞大的数据量对于各联盟链组织来说，将会带来很大的负担，因此通过账本数据的分布式存储、数据归档和老化、轻节点等方式减少数据量，将成为应对存储压力的主要方向。

趋势 3：安全和隐私保护的重要性愈加突出

区块链应用离不开数据的支撑，在监管机构对数据权属与治理意识不断增强的背景下，安全要求会不断强化，如何确保区块链信息系统的安全性，保护用户在链上数据不被非法访问，将会越来越重要。在密码学方面，国密算法逐渐成为联盟链的标准配置，各大区块链平台厂商都适配了国密证书、国密传输协议等技术方案，结合国内品牌的硬件和操作系统，以此提升系统的安全可控能力。

对于链上数据的隐私保护，越来越多的联盟链平台通过提供同态加密、群环签名、零知识证明、安全多方计算等技术能力，实现交易参与方的身份匿名和交易内容的隐私保

护。但单纯密码学的隐私保护方案面临着性能不足的问题，因此也有部分平台厂商通过软硬件结合方式，利用可信执行环境对交易敏感信息进行保护，在可信执行环境内部对数据进行明文运算，从而大幅提升隐私交易的性能。

但另一方面，在保证链上数据隐私的情况下，如何解决可监管的问题，仍是行业不断研究的方向。

趋势 4：链外协同和互操作打通“数据孤岛”

当前各区块链平台厂商主推的区块链产品在基础框架层及协议层各不相同，同时出于一些商业利益的考虑，也存在同一个业务由不同层级的主体在分别建设，随之带来了区块链时代的“数据孤岛”。

随着区块链覆盖范围的拓展，数据交换、共享粒度的加大，同一业务不同主体的数据打通，不同业务之间的数据协同，未来不同区块链业务平台间的互操作性必不可少。支持多云部署、跨链能力、提高兼容性会是未来区块链技术逐步推广后的主要诉求。

高效通用的跨链技术是实现万链互联的关键，跨链技术能够连通分散的区块链生态，成为区块链时代的 Internet。业界在跨链领域已经有大量的探索和积累，跨链技术正成为业界技术发展的热点方向。

另一方面，传统信息系统与区块链系统之间的数据交互诉求也会越来越突出。区块链系统需要通过链下系统扩展计算和存储能力，链下系统需要与区块链对接以解决信息可信、防篡改等问题。

趋势 5：学习成本大幅降低，用户体验更加友好

随着联盟链核心技术逐步过渡到相对成熟稳定的阶段，行业着力对区块链的部署运维体验进行优化，BaaS 平台厂商基于云基础设施搭建区块链平台框架，提供统一的应用程序编程接口、多语言软件开发工具包，便捷的区块链创建、管理、资源使用监控、运维等功能，保证了区块链系统稳定可靠，服务可用。

考虑到企业、政府、金融机构客户已有的 IT 信息系统的对接和集成，提供底层关系型数据库的支撑能力，并在编程接口层提供易用的 SQL API，使得用户可以无须感知底层技术的变化，仍然像使用数据库一样使用区块链。

为了更进一步降低用户的学习成本，也有部分厂商开始考虑提供可视化编程能力，通过拖拽等方式，实现区块链智能合约的功能开发、验证、调试、上线等能力。

4.2.2 区块链与周边技术深度融合

1. 区块链与云计算

云计算通常是指为企业、个人客户提供用来进行开发测试生产的计算、存储、网络等资源。在过去的 10 年间，云计算让传统信息行业变得前所未有的便捷。利用云计算所提供的服务，开发者只需要进行简单的工作，就可以完成在过去需要投入大量研发和运营时间成本的任务。目前市场上存在很多云服务架构，比如基础设施即服务（IaaS）、平台即服务（PaaS）、软件即服务（SaaS）。用户可以利用 IaaS 获得可伸缩的基础设施资源，利用 PaaS 方便地在线管理开发应用，利用 SaaS 使用网络软件。

云计算为区块链提供了底层的 IaaS 资源。区块链 BaaS 平台厂商基于云基础设施搭建区块链平台框架，提供统一的应用程序编程接口、多语言软件开发工具包，便捷的区块链

创建、管理、资源使用监控、运维等功能。应用集成商基于 BaaS 平台服务开发智能合约与 IT 系统进行对接，实现业务与区块链的深度融合。

也有观点认为，云计算使得区块链变得趋于中心化。但这里要说明的是，云计算虽然由某个云计算公司来负责运行和管理，但其本身仍然是一种典型的分布式的技术，通过云计算，把大量的集中式的应用系统变成了分布式的应用系统，云计算的中心化仅仅体现在统一的运行运营管理。当然，在联盟链中，不同的组织机构也可以选择不同的云计算提供商，来打消这方面的疑虑和担忧。

2. 区块链与大数据

大数据是生产资料，人工智能是生产力，区块链是生产关系。

大数据技术的目的是通过对数据的深度挖掘来发现问题，进而制定规则；而在区块链则为数据挖掘提供可信的数据支撑。区块链的分布式存储特性使得数据存储的可靠性比集中式的存储方式更强，共识机制确保链上数据的真实准确，链式结构使得数据变得可追溯，被篡改的风险变得更小，从而使得区块链在数据的安全性和数据质量方面具备其他技术难以比拟的优势。结合链外协同和链间的互操作，有利于将分散的“数据孤岛”联系起来，使得数据的分享和更大规模的数据挖掘成为可能。

可以预见的是，大数据的规模会随着区块链技术的发展而变得越来越大，不同业务场景的区块链数据融合连接，将进一步扩大数据的丰富性，帮助大数据发挥出更大的价值。

3. 区块链与 AI

人工智能的三大要素是算法、算力、数据。在“数据”维度上，区块链可以解决 AI 应用中数据可信度问题，同时通过链外协同和链间的互操作，有利于组织更大规模的数据，使得 AI 能够更加聚焦于算法。

在应用方面，AI 负责自动化的业务处理和智能化的决策，区块链负责在数据层提供可信数据，同时，区块链中的智能合约也是一段实现某种算法的代码，既然是算法，那么 AI 就能够植入其中，使区块链智能合约更加智能。

从另一角度来看，AI 模型的可解释性和可验证性也一直是一大痛点，将 AI 引擎训练模型结果和运行模型存放在区块链上，能够确保模型可验证，以及模型不被篡改，提升了模型的可信度，同时也降低了 AI 应用遭受攻击的风险。

4. 区块链与物联网

区块链只解决了链上数据的安全可信，但对于数据上链之前是否可信，却无法提供保证。在区块链解决方案中，通常使用预言机从链外获取信息并提供给链上的智能合约。物联网设备有望为数据可信上链提供更便捷可信的有效手段。

区块链能为物联网终端提供身份标识，明确数据权属，并提供数据价值交换的基础环境，实现数据源头的可信保障。如物流场景中，如果可以使用 GPS 定位技术将货物的实时位置记录上链，则可以省去大量的人工录入成本。通过在物联网终端设备上使用可信硬件技术，同时部署可信数据上链能力，将有望解决上链前数据可信的问题。

另一方面，考虑到物联网的发展趋势，未来终端与终端之间的直接通信将成为趋势，使得在一个局部网络内，可以利用区块链实现自治型的物联网系统，应用于无人机集群、车联网等业务场景中。

区块链与物联网结合，将有助于打造可信数据网络，催生出诸如分布式智能等新的应用场景，推动数据市场化进程。

5. 区块链与边缘计算

云计算作为中心化的计算，然后把中心化的计算再往外延伸，叫做边缘计算。在区块链应用中，可以将智能合约的运行节点部署在离用户很近的网络节点上，使得交易的验证和执行效率得到大幅提升；也可以将个人设备，比如，路由器或机顶盒设备里的存储空间贡献出来，并通过激励机制让个人用户参与到区块链分布式存储的网络中。

5. 总结

被誉为“数字经济”之父、《区块链革命》的作者唐·泰普斯科特（Don Tapscott）讲到的：“区块链代表着互联网的第二个时代，它将深刻改变行业”。未来随着数字经济的发展，区块链将作为新型基础设施推动互联网向下一代可信互联网演变，这将打破传统企业边界的限制，传统的商业模式也将发生深刻改变。虽然这些变化将推动社会经济的发展，但是过程是艰难的，要求我们必须投入大量的资源去夯实基础设施，作为坚实的底座来承载快速发展的可信业务需求与变化，这也正是华为区块链助力数字经济快速发展的定位与目标。

互联网是人类信息传递的基础设施，而区块链是互联网技术的发展和延续，如果把互联网比作信息之路，那么区块链的目的就是为它加上红绿灯、照明设施、信号标志等，让信息之路更安全可信。通过互联网技术实现了信息的流通，而通过区块链则可以实现价值的流通。信息流通过半自动化提升了生产生活效率，而价值流通将和机器智能、IOT、5G 等技术一起实现全自动化的智能社会，将进一步推动生产力发展。因此，区块链不是单一的系统和方法，需要通过纵向与横向的技术融合与开放发展，实现数据与价值在数字网络中的可信流转。

数据是数字经济的生产资料，而数据的可信传递是区块链构筑可信的根本。构筑端端的可信价值传递，需要围绕区块链为核心，融合 IOT、AI、5G、ROMA 等技术形成融合技术体系，方能保障数据从接入到应用的安全与可信，方能真正促进数字经济的快速发展。基于融合技术体系的区块链基础设施必将扩大信任的范围，降低信任成本，使得大规模实体间高效、可信的协作成为可能。区块链正在以前所未有的速度发展并影响着我们的生活，改变着当前的商业模式，所以区块链基础设施建设需要秉持开放的发展观点。我们相信，随着数据可信的不断发展，融合开放的区块链基础设施无疑将成为承担可信传递的基础网络设施，而与之伴随的，是基于价值的可编程社会、全面自动化的智能社会成为现实。