高等职业教育新目录新专标
电子与信息大类教材

区块链部署与运维

武春岭　卢建云　主　编
陶亚辉　智谷星图　李　腾　副主编
杨天若　主　审

電子工業出版社
Publishing House of Electronics Industry
北京 · BEIJING

内 容 简 介

本书力图系统、详细和通俗地介绍区块链部署与运维技术，目的是推动区块链技术应用专业的教学、研究和应用。本书以区块链基础、区块链平台、区块链平台部署、区块链平台监控为主线，内容涵盖区块链的基本概念、运行原理、数据结构、以太坊平台、FISCO BCOS、智能合约、区块链网络通信、区块链平台维护和监控等。本书在系统介绍区块链理论知识的基础上，结合丰富的案例进行操作实践的讲解，力求使读者在实践中深入理解区块链技术，具备主流区块链平台的部署与运维能力。本书对接区块链技术相关的国家职业技能标准要求，同时编者与区块链一流企业合作开发，建立教材资源动态更新机制。

本书可作为高等职业院校区块链技术应用专业及区块链相近专业的教材，也可作为区块链技术爱好者的参考用书。

图书在版编目（CIP）数据

区块链部署与运维 / 武春岭，卢建云主编. —北京：电子工业出版社，2023.6
ISBN 978-7-121-45849-1

Ⅰ. ①区… Ⅱ. ①武… ②卢… Ⅲ. ①区块链技术 Ⅳ. ①TP311.135.9

中国国家版本馆 CIP 数据核字（2023）第 115566 号

责任编辑：左　雅
印　　刷：
装　　订：
出版发行：电子工业出版社
　　北京市海淀区万寿路 173 信箱　邮编：100036
开　　本：787×1092　1/16　　印张：12　　字数：307 千字
版　　次：2023 年 6 月第 1 版
印　　次：2023 年 6 月第 1 次印刷
定　　价：45.00 元

凡所购买电子工业出版社图书有缺损问题，请向购买书店调换。若书店售缺，请与本社发行部联系，联系及邮购电话：（010）88254888，88258888。

质量投诉请发邮件至 zlts@phei.com.cn，盗版侵权举报请发邮件至 dbqq@phei.com.cn。

本书咨询联系方式：（010）88254580 或 zuoya@phei.com.cn。

前　言

区块链作为一种交叉的、综合性的技术，能够在陌生的环境中建立信任机制，颠覆了人们对传统技术的理解。区块链与物联网、大数据、云计算、5G 通信、人工智能等新一代信息技术的融合创新发展正在重塑我们的社会、经济和认知。区块链本身的去中心化、不可篡改、可追溯、集体维护、公开透明等特点，被认为在金融、征信、经济贸易结算、资产管理等众多方面拥有广阔的应用前景。区块链技术目前尚处于快速发展的初级阶段，现有区块链系统的设计和实现利用了分布式系统、密码学、共识算法、网络协议等学科知识，多学科的综合知识给区块链学习带来了很多困难。

近年来，高等职业教育专业目录中设置了区块链技术应用、区块链技术专业，但目前特别缺乏针对职业教育区块链技术应用专业的教材。本教材是结合国家区块链应用操作员职业技能标准和“岗课赛证”的理念而编写的。本教材聚焦区块链平台的运维技术，希望在不深入探讨区块链底层原理和算法的情况下，能够让读者通过实践理解和掌握区块链技术。

本书由重庆电子工程职业学院武春岭、卢建云担任主编，常州信息职业技术学院陶亚辉、智谷星图公司、重庆电子工程职业学院李腾担任副主编，海南大学杨天若（加拿大工程院院士、加拿大工程研究院院士、欧洲科学院院士）担任主审。具体分工：单元 1 由武春岭编写，介绍区块链基础知识，讨论区块链技术的概念、特性、技术架构和典型应用；单元 2 由卢建云编写，介绍区块链数据结构构建，包括区块结构、Merkle 树和区块数据存储；单元 3 由智谷星图公司编写，介绍以太坊、以太坊客户端和以太坊开发环境；单元 4 由智谷星图公司编写，介绍区块链平台部署，包括平台的背景、平台网络部署和平台的网络维护；单元 5 由卢建云编写，介绍智能合约应用；单元 6 由卢建云编写，介绍区块链网络通信，包括网络通信模型、RPC 协议和 P2P 网络搭建；单元 7 由智谷星图公司编写，介绍区块链平台维护，包括 FISCO BCOS 平台和 Hyperledger Fabric 管理工具；单元 8 由李腾编写，介绍区块链平台监控相关内容。

区块链是一门涉及多学科交叉的技术。编者深知要编写一本合适的教材并非易事，但希望本书通过聚焦区块链部署与运维技术为读者学习区块链带来帮助。然而，由于时间和水平的限制，书中难免有疏漏之处，还望读者批评指正。

编　者

2023 年 5 月

目　　录

单元 1　区块链漫游

学习目标

通过本单元的学习，使学生能够掌握区块链的概念、特性及分类，了解区块链的由来及发展里程碑，熟悉区块链的三种类型及应用场景。

任务 1.1　认识区块链

任务情景

【任务场景】

随着“新基建”的谋划布局和国家产业结构的调整，新产业、新业态、新模式亟待开拓，区块链需进行相应的产业变革和升级，不断扩大应用范围，逐步实现技术与产业的深度融合与创新发展，从而达到区块链与“新基建”的融合集成应用，构建数字经济高质量创新发展。那么，区块链与“新基建”有什么关系？区块链如何助力“新基建”？

【任务布置】

（1）学习区块链概念。
（2）学习区块链特性。
（3）学习区块链由来。
（4）学习区块链发展里程碑。
（5）学习区块链发展机遇与挑战。
（6）学习区块链如何助力“新基建”。

知识准备

1.1.1　区块链概念

2008 年 10 月 31 日，中本聪（Satoshi Nakamoto）发表一篇题为《比特币：一种点对点

式的电子现金系统》的论文，标志着不需要交易双方互信就可以安全交易的点对点价值交换体系的诞生。区块链的概念是从比特币系统的结构中抽象出来的，本质上是一个分布式账本。

传统的记账方式大多基于中心化结构，具有绝对地位的特权节点独立记账，其他节点服从于特权节点的权威，从而达成集体共识，共同维护此中心化结构记账系统的稳定。然而，中心化结构存在中心节点作恶、中心节点负载过高等问题，无法保证绝对信任可靠。去中心化结构，也叫分布式结构，通过每个节点都执行记账任务来保证只要大于 51%的节点是诚实的，那么记账结果一定是真实可靠的。

采用分布式结构的缺点在于账本信息的冗余程度较高，每个节点都需要独立维护一份账本，存储成本和计算成本都很高。同时分布式账本在节点记账权需要通过一定的规则进行分配，以保证系统不会出现恶性争夺或不顺从指挥等问题，这个规则称为共识机制。例如比特币中的共识机制为“工作量证明”（Proof of Work），通过与节点所拥有的算力成正比的概率轮流获取记账权，保障了比特币系统的稳定运行。

节点之间达成共识是通过 P2P 网络实现通信的，而不是通过传统中心化的服务器统一进行信息交换的。交换的信息包括刚刚产生的交易和已经打包为区块结构的交易。刚刚产生的交易通过“洪水算法”告知每个节点，而最近取得记账权的节点将其验证过合法性的交易列表打包为区块结构，并告知其他节点。所有节点对于这个新区块的合法性进行独立检查，如果符合要求，就将新区块放到所有合法区块的后面，通过链表式的结构连接起来，于是称为区块链。

总的来说，区块链是一种全新的融合型技术，存储上基于块链式数据结构，通信上基于点对点对等网络，架构上基于去中心化的分布式系统，交易上基于哈希算法与非对称加密技术，维护上基于共识机制。区块链作为一种多方共享的技术，融合了计算机科学、社会学、经济学、管理学等学科，实现了多个主体之间的分布式协作，构建了信任基础。

【课堂训练 1-1】请简述区块链的概念。

1.1.2 区块链特性

区块链具有五大基本特性，分别是去中心化、不可篡改性、开放性、匿名性和自治性。下面详细阐述每个特性的含义。

1. 去中心化

去中心化是指众多节点均具有平等的地位，没有永久性的特权节点，只有临时主导记账的节点。无论是存储还是计算任务，都由全部节点分别独立承担，以信息冗余、处理复杂度增加等代价换取了系统的可靠性和稳定性。点对点的交易系统通过密码学等数学算法建立信任关系，不需要第三方进行信任背书，从而彻底改造了传统的中心化信任机制。

2. 不可篡改性

信息一经打包为区块并加入区块链的最长合法链，就永久地被记录在区块链上。从概率学角度分析，几乎没有篡改或者删除链上信息的可能，除非恶意节点超过 51%，并集体作恶篡改数据库。通过区块链的巧妙设计，结合哈希算法、非对称加密等技术，衍生出应用潜力广泛的不可篡改特性，成了构建信任的重要基础。

3. 开放性

区块链系统是相对开放的。对于公有链，所有人都可以申请成为本区块链的一个节点。而对于联盟链和私有链，尽管需要经过一定的身份审核，但是一旦成为正式节点，所有的权利和义务均与其他节点平等，共同分享数据和接口。所有数据公开透明，查询内容真实可靠，应用开发规范清晰。

4. 匿名性

尽管区块链的所有数据是公开透明的，但是用户的隐私依然能够得到保护。区块链借鉴非对称加密技术中公私钥对的设计，将私钥作为用户的核心隐私，对外接收、发送转账只需暴露公钥，从而让交易对方无从获取其真实身份。另外，公私钥对可以无限次重复生成，一个用户可以拥有多个账号，这也为用户真实身份和交易信息的保护提供了保障。

5. 自治性

去中心化的结构导致区块链中节点的独立性很高，但是独立性不代表充分自由，不遵守区块链协议和规范的节点往往会受到惩罚。区块链通过全体节点协商一致的规则维护了区块链的安全性和稳定性，通过区块链社区的自行治理，不断完善规则，帮助区块链达成既定目标。

【课堂训练 1-2】区块链有几个特性？请简述每个特性的具体含义。

1.1.3　区块链由来

在遥远的旧石器时代，“货币”一开始是实物货币，如贝壳、金银等，因为它们具有稀缺性，因此可用于充当一般等价物。人们的记账方式也较为简单，普遍依靠死记硬背和心算。随着部落人数的增长和生产力的提高，开始出现生产剩余，人们就发明了用不同的符号来刻画记录和把场景画下来这两种方法记账。此后，结绳记事、书契等文字记录法，都是账本最初的形态。

后来，我们开始用纸币进行支付，比如 100 元面额的人民币的制作成本可能只有几毛钱，却能够换取价值 100 元的物品。这是因为有国家的信用背书，让人民相信这本来一文不值的纸币能够换 100 元的商品。

随着互联网的发展，我们从纸币过渡到记账货币。比如发工资只是在员工银行卡账号上做数字的加法、买衣服消费只是做减法，整个过程中都是银行在记账，且只有银行有记账权。但是这种记账方法仍然存在着信息不对称和信用问题。在 2008 年全球经济危机中，美国政府因为有记账权所以可以无限增发货币，将金融风险转嫁至其他国家。美联储可以为所欲为，通过无限量印钞来救市，也预示着在市场经济条件下法定货币信用的不确定性。

2008 年，比特币的创造者中本聪创建了一种新型支付体系：大家都有权利进行记账，货币不能超发，整个账本完全公开透明，十分公平，这就是比特币产生的原因和动机。

这种分布式账本可以完美解决以上记账方法的不足，它由一个甚至多个甚至无数个区块组成，假设每个区块代表账本的一页，区块可以无限增加，每个区块都会加密并盖上时间戳，按照时间顺序链接成一个总账本，由参与用户共同维护。区块链技术可以很好地解决信任成本问题，带来了一种智能化信任。与最初的账本不同的是，这种智能化信任是建立

在区块链上的，而非由单个组织掌控，从而使公信可以被多方交叉验证与监督。

区块链的首次出现是在 2008 年的“比特币白皮书”《比特币：一种点对点的电子现金系统（*Bitcoin A Peer-to-Peer Electronic Cash System*）》中。中本聪在文中描述了比特币的概念及其工作机制。然而，中本聪在这篇文章中并未直接使用区块链（BlockChain）这个术语，中本聪将这项技术描述为，每个区块都包含关于事务的数据，所有区块都连接在一个链中。多年后，区块链成了这项技术的术语，但如上所述，中本聪从未这样称呼它。

区块链的整体技术发展需要依靠多种核心技术的整体突破，这些技术主要包括分布式存储、P2P 技术、非对称加密技术、共识机制等。

虽然中本聪是最早提出使用区块链记录比特币交易的人，但从技术上讲，这并不是区块链概念的开始。为此，我们必须追溯到 1991 年，在斯图尔特·哈伯（Stuart Haber）和斯科特·斯托内塔（W. Scott Stornetta）撰写的题为《如何在数字文档上加盖时间戳（*How to Time-Stamp a Digital Document*）》的一文中，第一次提出关于数据区块的加密保护链产品。文中，二人提出了加盖时间戳的数字文档的概念，以确保交易在某个时间“签署”。次年，哈伯和斯托内塔在每个“块”中应用了默克尔树（Merkle Tree），也称为哈希树（Hash Tree），来存储交易数据。

1996 年，剑桥大学的一位密码学家罗斯·安德森（Ross Anderson）在论文中描述了一个无法删除和篡改任何对系统所做的更新的分布式存储系统。在当时，这被认为是一篇关于开发更安全的点对点系统的革命性论文。2000 年，斯特凡·康斯特（Stefan Konst）发表了加密保护链的统一理论，该理论针对文件签名的匿名性和安全性提出了一整套实施方案。

区块链技术的一个重大突破发生在 2002 年，当时的密码学家大卫·马齐尔（David Mazières）和丹尼斯·莎莎（Dennis Shasha）提出了一个分散信任的网络文件系统。这是区块链技术的原型，这个文件系统的作者之间相互信任，而不是信任系统本身。他们使用 SHA256 加密或类似的哈希函数进行数字签名，提交并将其附加到默克尔树中的其他链中。

这些技术最终实现了信息的不可篡改性和在保密的前提下被更多人认证的区块链技术体系，并且开始在应用领域创造奇迹。其更为重要的应用价值是，可以使原本互不信任的各方借此迅速建立相互信任的合作关系。

【课堂训练 1-3】请简述区块链的由来。

1.1.4 区块链发展里程碑

区块链的发展经历了三个里程碑，分别是区块链 1.0、区块链 2.0 和区块链 3.0。下面详细介绍这三个里程碑。

1. 区块链 1.0：从比特币看区块链

区块链 1.0 是以比特币为代表的虚拟货币的时代，代表了虚拟货币的应用，包括其支付、流通等虚拟货币的职能，目标是实现货币的去中心化与数字货币交易支付功能。

比特币就是区块链 1.0 最典型的代表，区块链的发展得到了欧美等国家市场的接受，同时也催生了大量的货币交易平台，实现了货币的部分职能，能够进行货品交易。比特币勾勒了一个宏大的蓝图：未来的货币不再依赖于各国央行发行，而是进行全球化的货

币统一。

虽然区块链 1.0 的蓝图很庞大，但是无法普及到其他行业中，因此区块链 1.0 只能满足虚拟货币的需要。区块链 1.0 时代也是虚拟货币的时代，也涌现出了大量的山寨货币等。

2. 区块链 2.0：以太坊与通证

区块链 2.0 是指智能合约。智能合约与货币相结合，为金融领域提供了更加广泛的应用场景。一个智能合约是一套以数字形式定义的承诺，合约参与方可以在上面执行这些承诺的协议。

区块链相对于金融场景有强大的天生优势。简单来说，如果银行进行跨国的转账，可能需要面对打通各种环境、货币兑换、转账操作、跨行问题等。而区块链实现的点对点操作，避免了第三方的介入，直接实现点对点的转账，提高了工作效率。

区块链 2.0 的代表是以太坊。以太坊是一个平台，它提供了各种模块让用户来搭建应用平台之上的应用，其实也就是合约，这是以太坊技术的核心。以太坊提供了一个强大的合约编程环境，通过合约的开发，以太坊实现了各种商业与非商业环境下的复杂逻辑。以太坊的核心与比特币系统本身是没有本质区别的，而以太坊是智能合约的全面实现，支持了合约编成，让区块链技术不仅仅是虚拟货币，而是提供了更多商业、非商业的应用场景。

3. 区块链 3.0：去中心化应用

区块链 3.0 是指区块链在金融行业之外各行业的应用场景，能够满足更加复杂的商业逻辑。区块链 3.0 被称为互联网技术之后的新一代技术创新，足以推动更大的产业改革。

区块链 3.0 涉及生活的方方面面，所以区块链 3.0 将更加具有实用性，赋能各行业，不再依赖于第三方或某机构获取信任与建立信用，能够通过实现信任的方式提高整体系统的工作效率。

换言之，区块链 1.0 是区块链技术的萌芽，区块链 2.0 是区块链在金融、智能合约方面的技术落地，而区块链 3.0 是为了解决各行各业的互信问题与实现数据传递安全性的技术落地。

【课堂训练 1-4】请简述区块链发展的三个里程碑。

1.1.5　区块链发展机遇与挑战

1. 发展机遇

随着区块链技术在全球各行业的迅猛发展，市场对专业人才的渴求剧增，人才供需失衡成了行业热点问题。前不久，中国电子学会《区块链技术人才培养标准》（以下简称《标准》）推出了区块链技术人才岗位群分布整理和学科培养内容体系建议，为未来全国范围的区块链技术人员的人才培养和能力测试做了纲领性引导。

据了解，区块链技术近两年来呈现爆发趋势，对人才的需求也急剧增长，从传统互联网行业流入的技术人才无法满足人才市场需求，造成了人才与需求的脱轨。市场上也出现形式多样的区块链技术培训，大量无主体、不规范的培训班在市场上显现，呈现人才培养伪速成的现象，成为区块链行业虚荣性泡沫中的一大问题。

由于区块链技术开发的核心是将现有技术应用到新的逻辑架构中进而实现新功能，所

以区块链人才招募并非技术门槛高，而是同时拥有复合型技术知识和区块链实际开发经验的人才存量有限。事实上，目前区块链人才市场已整体降温，人才供需比趋于理性。据悉，目前行业逐渐回归理性，无论是薪资待遇还是岗位需求均有所下降。但是区块链人才仍然是稀缺的，主要表现为对区块链人才由量向质的需求转变，企业对区块链人才提出了更高的要求。区块链技术的各个模块需要多种专业领域知识。其中，数据结构为网络服务、数据存储、权限管理、共识机制、智能合约等模块共同需要，成为适应性最广的专业领域。

越来越多的区块链应用出现在我们的日常生活中，下面从金融服务、征信和权属管理、共享经济、国际贸易、数字版权这五个方面阐述区块链未来的发展方向和应用场景。

（1）金融服务。区块链技术能够在没有第三方信用背书的情况下降低交易成本，减少跨组织交易风险。全球不少银行、金融交易中心都在研究区块链技术，还有一些投资机构也在利用区块链技术降低管理成本、提高资金流动效率和降低管控风险。

（2）征信和权属管理。征信和权属的数字化管理是大型社交媒体平台和金融平台梦寐以求的。区块链被认为可以促进数据交易和流动，并提供安全可靠的支持。当然，征信行业的门槛比较高，需要多方资源的配合与推动。

（3）共享经济。以 Uber、滴滴、Airbnb 为代表的共享经济现有的模式将会受到去中心化应用的冲击，目前大的中心机构虽然提供了更可靠的服务和信用，但一旦中心化机构获得了垄断地位，其昂贵的费用不仅让服务提供方不满，服务的接收方也会颇有怨言。而去中心化应用可以降低信任成本，提高管理效率。这个领域主题相对集中，应用空间广泛，因此受到大量投资者的关注。而该领域的难点在于如何在用户体验上做到与中心化共享经济平台相媲美。

（4）国际贸易。区块链技术可以帮助简化自动化国际贸易和物流供应链领域中烦琐的手续和流程。基于区块链设计的国际贸易方案将会为参与的多方企业带来极大的便利。国际贸易中销售和法律合同的数字化、货物监控、货物溯源、货物检测、实时支付等方向都可能成为创业的突破口。

（5）数字版权。从本质上来说，区块链技术能够带来生产关系的变革，而数字资产是最容易通过区块链技术进行高效流转的。未来将会出现去中心化的音乐平台、电影平台、小说平台及其他一些数字版权平台，这些数字内容的作者可以将属于自己的音乐、影视、小说等的版权放在公开透明的去中心化数字版权平台上，只要有用户购买其版权作品，作者就可以实时地自动获得其版权收益，中间不需要通过平台来进行分发和抽取利润分成。

同时，我国十分重视区块链技术的发展和运用，不仅在中央决策层面有引导政策，在各地方也有产业支持的相关规定。

2016 年 12 月，国务院下发的《“十三五”国家信息化规划的通知》中首次将“区块链”作为战略性前沿技术写入规划。

2018 年 4 月，教育部发布《教育信息化 2.0 行动计划》，提出积极探索基于区块链、大数据等新技术的智能学习效果记录、转移、交换、认证等有效方式，形成泛在化、智能化学习体系，推进信息技术和智能技术深度融入教育教学全过程。

2018 年 6 月，网信办发布《区块链信息服务管理规定》，为区块链信息服务的提供、使用、管理等提供了有效的法律依据。

2018 年 6 月，工信部发布《工业互联网发展行动计划（2018—2020 年）》，鼓励推进区

块链、边缘计算、深度学习等新兴前沿技术在工业互联网中的应用研究。

2019 年 10 月 24 日，中共中央政治局就区块链技术发展现状和趋势进行第十八次集体学习，习近平总书记在主持学习时强调，要把区块链作为核心技术自主创新的重要突破口，明确主攻方向，加大投入力度，着力攻克一批关键核心技术，加快推动区块链技术和产业创新发展。区块链行业从业者将这一次习近平总书记的重要表述称为“1024 讲话”，这次讲话深刻地改变了区块链行业，为区块链行业的发展带来了新动能。

2021 年 3 月，十三届全国人大四次会议表决通过了《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》（以下简称“十四五”规划）。在区块链产业具体内容上，“十四五”规划提出：推动智能合约、共识算法、加密算法、分布式系统等区块链技术创新，以联盟链为重点发展区块链服务平台和金融科技、供应链管理、政务服务等领域应用方案，完善监管机制。

2. 未来挑战

区块链在未来发展过程中也面临着一些挑战，下面主要从安全、人才、观念、标准和法律等方面阐述区块链面临的挑战。

1）安全

区块链是基于密码学、点对点通信、共识算法、智能合约、顶层应用构建等技术的融合型技术，因此针对每个采用的技术，都存在一定的安全风险。

（1）密码学包括哈希算法、非对称加密等加密解密技术，一些密码学算法本身就存在漏洞。对于一些成熟的密码学算法，如比特币所采用的 SHA-256 算法和椭圆加密算法，尽管目前尚不存在破解方法，但是随着量子计算的不断发展，计算力的指数级提升可能会对所有现有密码学算法带来冲击。为此，应当继续探索对抗量子计算的量子密码学算法。同时，公私钥对的账号模式对私钥的安全性提出了挑战，传统钱包软件能否安全保护用户私钥还不可知，用户能否妥善保管私钥也是一大安全隐患。

（2）对于点对点通信网络，有五种常见攻击方式对区块链安全造成冲击。第一，日食攻击。日食攻击是通过建立大量的恶意连接来使得某个节点被孤立、被隔离在恶意网络中，恶意节点垄断此节点的输入和输出，诱骗其执行恶意节点的任务或者使其误以为已经发生转账从而盗取钱财。第二，分割攻击。攻击者利用边界网关协议（BGP）改变节点消息的路由途径，从而将整个区块链网络分割为两个或多个，待攻击结束后，区块链重新整合为一条链，其余链将被废弃，从而使攻击者选择将对自己最有利的部分变为最长链，实现“双重支付”“恶意排除交易”等非法行为。第三，延迟攻击。攻击者通过边界网关协议控制对某些节点的新消息接受，从而延迟其挖矿监听的时间，使得矿工损失大量挖矿时间和算力。第四，DDoS 攻击。攻击者通过发送大量恶意消息并且不进行握手确认，占用大量接收信息节点的计算存储资源和网络通信资源，从而使得区块链网络瘫痪。第五，交易延展性攻击。多数挖矿程序是用 Openssl 库校验用户签名的，而 Openssl 兼容多种编码格式，所以对签名进行微调依然是有效签名。攻击者通过微调签名并且使用不同的交易 ID 实现对同一笔交易的“双重支付”行为。

（3）针对共识算法层面，常见的攻击方式主要有两种。第一，51%攻击。51%攻击主要针对 PoW 算法，如果系统恶意节点掌握了超过 51%的算力，那么大概率有能力控制最长

合法链的强制选择，从而使得任何恶意交易都可以变得“合法”。第二，女巫攻击。攻击者通过单一节点生成大量假名节点，通过控制大量节点并谎称完全备份来获得与其实际资源不匹配的强大权利，并削弱冗余备份的作用。另外，还有短距离攻击、长距离攻击、币龄累计攻击和预计算攻击。

（4）针对智能合约层面，目前针对合约虚拟机的主要攻击方式有逃逸漏洞攻击、逻辑漏洞攻击、堆栈溢出漏洞攻击、资源滥用漏洞攻击。同时，针对智能合约的主要攻击方式有可重入攻击、调用深度攻击、交易顺序依赖攻击、时间戳依赖攻击、误操作异常攻击、整数溢出攻击和接口权限攻击等。

（5）针对应用层，主要是数字货币交易平台、区块链移动数字钱包 App、网站、DAPP 等存在管理漏洞和技术漏洞问题。

2）人才

从 2008 年区块链概念问世至今，区块链已经经过了十几年的飞速发展，但是由于时间有限，社会认知困难，人才储备一直不足。区块链领域往往需要复合型人才，因为区块链不单纯是一个技术问题，更是业务模式创新的问题，所以要求从业人员对业务模式也有深入的认识和分析。

根据《2018 年区块链人才供需与发展研究报告》，真正具备区块链人才要求的人仅占总需求量的 7%。《区块链白皮书（2019）》也提出，区块链技术是一门多学科跨领域的技术，包含了密码学、数学、金融、操作系统、网络通信、社会生产等，但是我国目前在交叉学科方面有待进一步发展。

3）观念

区块链的概念在普及过程中遇到很大阻力，有以下两点原因。

第一，区块链本身是一个多学科融合、应用场景较为复杂的技术，所以对大众的知识水平有较高的要求。现在区块链概念普及的重要工作方向是如何让大众形象、真切地感受区块链的社会价值。

第二，区块链在过去的“币圈”发展中给大众带来了很多负面印象。“币圈”在全世界范围产生了深远的影响，尽管正面作用突出，但是各类盗窃、诈骗、投机等乱象层出不穷，在大众心中树立了区块链并不可靠的负面形象。“币圈”仅仅是区块链领域的一部分，由于其发展时间较短、标准尚未统一等问题，一直处于野蛮增长阶段。相信在行业规范诞生后，“币圈”能够逐步拥抱实体经济，脱虚向实，成为实体经济的内在价值流转机制，为社会做出安全可靠的贡献。

4）标准

区块链行业由于发展时间较短，各个企业组织往往“自起炉灶”，架构、网络通信、密码学算法、共识机制等标准的不同为互联互通带来了极大的障碍，从而影响区块链产业的落地进程。

区块链行业的标准统一将有助于大众充分认识区块链，有助于监管部门的有效监督，有助于行业企业的高速发展，能大大减少“重复造轮子”等社会资源浪费现象。目前国家和行业企业都在积极进行区块链行业标准的探索与沟通，这有利于我国在区块链技术上的自主创新，加速区块链产业互联互通。

（5）法律

区块链行业一方面有待完善相关法律法规，另一方面要严格遵守反洗钱、限制 ICO 等法律的规范，处于一个谨慎发展的阶段。法律层面应该对区块链底层技术和上层应用进行完善的规范，从账号安全、资金安全、隐私安全、软件安全、业务安全、存储安全、计算安全等方面进行严格监管，避免技术风险和道德风险。同时，需要继续理性控制数字货币的监管问题，在保护大众的同时引领我国在数字货币、数字资产领域的快速发展。

【课堂训练 1-5】请简述区块链的发展机遇与挑战。

任务实施

1.1.6　区块链如何助力“新基建”

“新基建”将加速中国经济社会的数字化进程，“新基建”的应用需要新的信任机制作为纽带，而区块链是构建未来数字基建的信任基石，将推动信息互联网升级到价值互联网，加速数字基建的进程，迎来全新而广阔的数字时代。

1. 物联网

物联网（Internet of Things，IOT），是传统互联网和电信网深度结合的产物，实现了独立物品个体的万物互联。物联网技术在社会中已经被深度应用，未来将形成现实世界的数位化。物联网技术在物流与运输、供应链管理、供应链金融、工业信息化、智慧城市、自动无人驾驶等方面有着广阔的应用前景。

虽然物联网近年来的发展渐成规模，但在发展演进过程中仍存在诸多难以攻克和解决的问题。

在个人隐私方面，中心化的管理架构无法自证清白，个人隐私数据被泄露的事件时有发生。在扩展能力方面，目前的物联网数据流都汇总到单一的中心控制系统，随着未来物联网设备呈几何级数增长，中心化服务成本难以负担，物联网网络与业务平台需要新型的系统扩展方案。在网间协作方面，目前很多物联网都是运营商、企业内部的自组织网络，涉及跨多个运营商、多个对等主体之间的协作时，建立信用的成本很高。在设备安全方面，缺乏设备与设备之间相互信任的机制，所有的设备都需要和物联网中心的数据进行核对，一旦数据库崩塌，会对整个物联网造成很大的破坏。在通信协作方面，全球物联网平台缺少统一的技术标准、接口，使得多个物联网设备彼此之间通信受到阻碍，并产生多个竞争性的标准和平台。

区块链凭借“不可篡改”“共识机制”“去中心化”等特性，将对物联网产生重要的影响。

（1）降低成本：区块链“去中心化”的特质将降低中心化架构的高额运维成本。

（2）隐私保护：区块链中所有传输的数据都经过加密处理，用户的数据和隐私将更加安全。

（3）设备安全：身份权限管理和多方共识有助于识别非法节点，及时阻止恶意节点的

接入和作恶。

（4）追本溯源：数据只要写入区块链就难以被篡改，依托链式结构有助于构建可证可溯的电子证据存证。

（5）网间协作：区块链的分布式架构和主体对等的特点有助于打破物联网现存的多个信息孤岛桎梏，以低成本建立互信，促进信息的横向流动和网间协作。

2. 大数据

2020 年 4 月，国家发改委在例行新闻发布会上，首次明确了“新基建”的范围，区块链被首次正式提及，同时被提及的还有大数据、人工智能。大数据主要是通过海量的数据进行机器学习，通过数据分析协助做出各种决策。而区块链在产业中的应用，第一步就是数据信息上链。区块链和大数据都是针对数据进行相应的处理，两者的区别与联系又在哪里呢？

大数据更多的是对源数据进行清洗、治理，目的是为了通过分析历史数据得出规律，便于未来决策。区块链的本质是分布式存储、非对称加密、P2P 网络等技术共同作用下的“技术组合”。“不可篡改”是由一组技术共同实现的，区块链在本质上不对数据进行任何加工处理，而是保证数据在区块链技术搭建的技术体系架构中可以进行真实记录，不被篡改。当然，“不可篡改”不等于“不能篡改”，根据不同的共识机制，当占用资源超过一定程度后，便可以进行篡改。例如，在 POW 的共识机制下，拥有超过 50%的算力的一方，就可以篡改数据。

大数据与区块链之间虽然有诸多区别，但也可以进行结合，相互形成有利的补充，去解决应用场景中的技术问题，发挥一加一大于二的效果，二者的结合也必然是未来技术发展的趋势之一。

第一，区块链为大数据收集和需要处理的数据提供相对更为科学的存储方式，以及存储多种类型格式的数据包容性。结合区块链的其他技术特性，保证了源数据的真实性。此特性是除区块链技术之外，当前其他技术不具备的。

第二，在通过大数据技术进行机器学习与建模之前，一般都会进行数据挖掘、数据清洗、数据治理的工作，且通常会进行跨系统、跨地域、跨技术架构的数据收集。在对数据进行治理之时，数据库表结构、数据格式、数据的安全机制等各不相同，区块链是一个包容性很好的数据存储工具，通过分布式存储，统一数据规范，且不受数据格式的限制，同时还可以保证源数据的真实性。因此，区块链是一个非常好的打破数据孤岛，实现数据共享的工具。

第三，在数据安全方面，区块链可以更加动态化、精细化、低成本地实现对数据访问不同权限的设置。还可以通过相应的非对称加密技术，对数据进行“脱敏”处理或只允许“机读格式”，以方便对内部保密数据和外部数据同时进行机器学习和数据建模。

综上所述，比较来看，区块链在数据存储方面发挥了更大的作用，而大数据在数据分析方面更有优势。大数据与区块链是两种不同的技术，但二者在数据层上有很大的互补性。大数据与区块链技术的结合，可以更好地发挥数据价值，起到价值传输、价值转化的作用。

3. 人工智能

人工智能是一门基于大数据的交叉科学，应用最广的领域包括智能机器人、语音语义识别、图像图片识别等。除了对数据进行分析处理这一与大数据领域类似的应用，人工智能还包括各种智能终端硬件设备，这也是物联网信息采集基础设施的重要组成部分。人工智能终端设备可以更方便、及时地采集数据，但却无法解决跨个体、跨系统的信任问题。区块链的分布式账本、共识机制，甚至匿名性，都有助于建立一个信任体系。信任的环境有助于推动数据加快汇集，从而深化数据的应用，推动人工智能的发展。因此人工智能与区块链技术的结合也必将使二者互相促进。

在算力方面，人工智能对算力需求很大。人工智能终端设备普遍分散分布，每个终端设备在条件允许的情况下，都可以作为分布式的计算节点，可以通过区块链的技术架构来分享算力，为人工智能提供支持。贡献算力即挖矿，可以激励分散的计算节点来贡献空闲算力，参照区块链中获得区块打包权的方式，将计算任务拆解分配给多个计算节点。

在算法方面，当需要算法保密或完全以私密的方式进行时，区块链的匿名性将发挥很大的作用。非对称加密技术保证了传输过程中的安全，方便分布式、多方同时提供数据训练模型。

由此可见，区块链与人工智能在底层技术方面也有诸多互补性，在不同的应用场景中，应当选择合适的方式将二者结合起来，使得二者的价值得到充分发挥，更好地解决应用场景与实际业务中的问题。

4. 云计算

区块链的本质就是分布式账本和智能合约。分布式账本是一个独特的数据库，这个数据库像网络一样，所有人都使用区块链就会建立一个生态系统。个人的分布式账本利用数学及密码学，可以永远记住固定序列，事实内容不会被篡改。而智能合约是交易双方互相联系来约定规则的，谁都不能更改。

从定义上看，云计算是按需分配，区块链是构建了一个信任体系，二者好像没什么直接关系。但是区块链本身就是一种资源，有按需供给的需求，是云计算的一个组成部分，云计算的技术和区块链的技术之间是可以互相融合的。

从宏观上来看，利用云计算已有的基础服务设施或根据实际需求做相应改变，实现开发应用流程加速，满足未来区块链生态系统中初创企业、学术机构、开源机构、联盟和金融等机构对区块链应用的需求。对于云计算来说，“可信、可靠、可控制”被认为是云计算发展必须要翻越的三座大山，而区块链技术以去中心化、匿名性，以及数据不可篡改为主要特征，这与云计算的长期发展目标不谋而合。

从存储上看，云计算的存储和区块链内的存储是由普通存储介质组成的。而区块链里的存储是链里各节点的存储空间，区块链里存储的价值不在于存储本身，而在于相互链接不可更改的块，是一种特殊的存储服务。云计算里确实也需要这样的存储服务，比如结合“平安城市”，将数据放在这种类型的存储里，利用不可篡改性，让视频、语音、文件等作为公认有效的法律依据。

从安全性上看，云计算里的安全主要是确保应用能够安全、稳定、可靠地运行。而

区块链内的安全是确保每个数据块不被篡改，数据块的记录内容不被没有私钥的用户读取。利用这一点，如果把云计算和基于区块链的安全存储产品结合，就能设计出加密存储设备。

许多区块链支持者认为其运作模式最适合云端。关于这个命题的想法是，虽然云计算本身是分布式和容错的，但仍然使用集中式方法来运行，中央实体负责云计算。由于在整个云“网络”中建立了多个数据库，区块链的分散性将提供更多的自主操作和更高级别的数据安全性。

堆积于区块链的云的一个限制是，由于分散化的结构，需要更高的安全性来控制节点间通信，从而需要使用高度安全的传输协议。而这些协议将会增加对物理和计算资源的需求，这可能使区块链交易比当今基于云计算的操作成本更加高昂。

区块链开发是一种比较新的方法，其发展似乎提供了潜在的发展和实施的安全性，其核心价值已经开始被金融机构所接受，一些大型银行已经开展了自己的试点项目。尽管其提供了分散环境和自动化各种数据中心功能的潜力，但这些功能在很大程度上仍然是投机性的。在不久的将来，寻求开发和实现自己的区块链应用的用户似乎属于主要云提供商的范围。区块链仍然处于发展的早期阶段，而这种应用开发的方法将具有一个扩展的成熟过程。

2018 年初，Facebook CEO 扎克伯格宣布探索加密技术和虚拟加密货币技术，国外的卫轩、亚马逊、谷歌、IBM 等也相继入场，国内的腾讯、京东、阿里巴巴等互联网巨头也都接连宣布涉足区块链，迅雷更是通过提前布局云计算与区块链实现了企业的转型与业务的快速增长。

布局 BaaS 领域的公司基本上都是大型的云计算服务商。在云的基础上，提供区块链技术主要基于三个方面：成本效率、因公生态、安全隐私。对于云服务商来说，一切硬件设施和基础架构都是现成的，降低 IT 成本已成为必然趋势，引入像区块链这样的新技术至关重要。其中以联盟链为代表的区块链企业平台，需要利用云设施完善区块链生态平台；以公有链为代表的区块链，则需要为去中心化应用提供稳定可靠的云计算平台。

任务评价

填写任务评价表，如表 1-1 所示。

表 1-1　任务评价表

工作任务清单	完成情况
学习区块链概念	
学习区块链特性	
学习区块链由来	
学习区块链发展里程碑	
学习区块链发展机遇与挑战	
学习区块链如何助力“新基建”	

任务拓展

【拓展训练 1-1】什么是比特币？比特币与区块链之间有什么关系？请简述比特币的工作原理。

任务 1.2　区块链分类

任务情境

【任务场景】

区块链包含三种类型：公有链、联盟链和私有链。其中，联盟链的网络范围介于公有链和私有链之间，通常使用在多个成员角色的环境中，比如银行之间的支付结算、企业之间的物流等。这些场景往往都是由不同权限的成员参与的，与私有链一样，联盟链系统一般也是具有身份认证和权限设置的，而且节点的数量往往也是确定的，适用于企业或机构之间的事务处理。联盟链并不一定要完全管控，如政务系统，有些数据可以对外公开，就可以部分开放出来。那么，如何实现联盟链？它的技术解决方案是什么？

【任务布置】

（1）学习区块链的分类。

（2）学习联盟链技术解决方案（超级账本）。

知识准备

使用区块链技术的根本目的是解决效率和信任问题，由于不同场景下的应用对象不同，因而开放程度、应用范围也存在差异。根据开放程度的不同，一般按照准入机制可将区块链分为公有链（Public Blockchain）、联盟链（Consortium Blockchain）和私有链（Private Blockchain）。

1.2.1　区块链的三种类型

1. 公有链

公有链对外公开，用户不用注册便能参与，能自由访问区块链上的所有信息。公有链是真正意义上的完全去中心化的区块链，通过密码学保证信息不被篡改，通过经济学上的激励，在匿名的 P2P 网络中达成共识，从而形成去中心化的区块链。

公有链是最早出现的区块链，也是应用最广泛的区块链，绝大部分虚拟数字货币均基于公有链，世界上有且仅有一条该币种对应的区块链。作为中心化或准中心化信任的替代

物，公有链的安全由共识机制来维护——共识机制可以采取 PoW 或 PoS 等方式，将经济奖励和加密算法验证结合起来，并遵循着一般原则：每个人从中可获得的经济奖励与对共识过程做出的贡献成正比。

公有链通常也称为非许可链（Permissionless Blockchain），如比特币和以太坊等都是公有链。公有链一般适合于虚拟货币、面向大宗的电子商务、互联网金融等 B2C、C2C 或 C2B 等应用场景。

在公有链中，程序开发者无权干涉用户，所以区块链可以保护使用他们开发程序的用户。从传统的经济学角度来看，的确难以理解为何程序开发者会愿意放弃自己的权限，然而，随着互联网崛起，协作共享的经济模式为此提供了两个理由：首先，如果你明确地选择做一些很难或者不可能的事情，其他人会更容易信任你并与你产生互动，因为他们相信那些事情不大可能发生在自己身上；其次，如果你是受他人或其他外界因素的强迫，无法去做自己想做的事，你大可用“即使我想，我也没有权力去做”的话语作为谈判筹码，这样可以劝阻对方不要强迫你去做不情愿的事。程序开发者们所面临的压力或者风险主要来自于政府，所以说“审查阻力”便是公有链最大的优势。

公有链具有如下特点。

（1）所有交易数据公开、透明。虽然公有链上的所有节点是匿名（“非实名”）加入网络的，但任何节点都可以查看其他节点的账号余额及交易活动。

（2）无法篡改。公有链是高度去中心化的分布式账本，篡改交易数据几乎不可能实现，除非篡改者控制了全网 51%的算力，以及需要巨额的运作资金。

（3）低吞吐量。高度去中心化和低吞吐量是公有链不得不面对的两难问题，例如最成熟的公有链——比特币区块链，每秒只能处理 7 笔交易信息（按照每笔交易大小为 250 字节估算），高峰期能处理的交易笔数就更低。

（4）交易速度缓慢。低吞吐量必然带来缓慢的交易速度。比特币网络极度拥堵，有时一笔交易需要几天才能处理完毕，还需要缴纳转账费。

2. 联盟链

联盟链是指其共识过程受到预选节点控制的区块链，由某个群体内部指定多个预选的节点为“记账人”，每个块的生成由所有的预选节点共同决定（预选节点参与共识过程），其他接入节点可以参与交易，但不过问记账过程（本质上还是托管记账，只是变成分布式记账，每个块的记账人成为该区块链的主要风险点），其他任何人可以通过该区块链开放的 API 进行限定查询。这些区块链可视为部分去中心化。

联盟链仅限于联盟成员参与，区块链上的读写权限参与记账权限按联盟规则来制定。由 40 多家银行参与的区块链联盟 R3 和 Linux 基金会支持的超级账本项目都属于联盟链架构。联盟链是一种需要注册许可的区块链，其共识过程由预先选好的节点控制。一般来说，它适合于机构间的交易、结算或清算等 B2B 场景，如在银行间进行支付、结算、清算的系统就可以采用联盟链的形式将各家银行的网关节点作为记账节点，当网络上有超过 2/3 的节点确认一个区块，该区块记录的交易将得到全网确认。联盟链可以根据应用场景来决定对公众的开放程度。由于与共识的节点比较少，联盟链一般不采用工作量证明的挖矿机制，而是多采用权益证明或 PBFT 等共识算法。联盟链对交易的确认时间和每秒交易数都与公

有链有较大的区别，对安全和性能的要求也比公有链高。

联盟链网络由成员机构共同维护，网络接入一般通过成员机构的网关节点接入。联盟链平台应提供成员管理、认证、授权、监控、审计等安全管理功能，如 2015 年成立的 R3 联盟，旨在建立银行同业的一个联盟链，目前已经吸引 40 多个成员，包括世界著名的银行（摩根大通、高盛、瑞信、巴克莱、汇丰等）和 IT 巨头（IBM、微软等）。

联盟链的特点是可以很好地进行节点间的连接，只需要极少的成本就能维持运行，提供迅速的交易处理服务和低廉的交易费用，有很好的扩展性（但是扩展性随着节点增加又会下降），数据可以有一定的隐私。当然缺点也很明显，联盟链意味着这个区块链的应用范围不会太广，缺少比特币的网络传播效应，而且联盟链容易造成权力集中。由于节点少，并且需要预选节点进行记账，联盟链不能完全解决信任问题，一旦运用不当就容易使权力集中，甚至引发安全问题。

联盟链具有如下特点。

（1）部分去中心化。与公有链不同，联盟链在某种程度上只属于联盟内部的成员所有，且很容易达成共识，因为毕竟联盟链的节点数是非常有限的。

（2）可控性较强。公有链是一旦区块链形成，将不可篡改，这主要源于公有链的节点一般是海量的。而对于联盟链来说，只要所有机构中的大部分达成共识，即可更改区块数据。

（3）数据不会默认公开。不同于公有链，只有联盟里的机构及其用户才有权限访问联盟链中的数据。

（4）交易速度很快。跟私有链一样，联盟链本质上还是私有链，因此其节点不多，容易达成共识，交易速度自然也就快很多。

3. 私有链

私有链是指其写入权限由某个组织和机构控制的区块链，读取权限或者对外开放，或者被进行了任意程度的限制。相关的应用可以包括数据库管理、审计等，尽管在有些情况下希望它能有公共的可审计性，但在很多的情形下，公共的可读性似乎并非是必需的。

大多数人一开始很难理解私有链存在的必要性，认为其和中心化数据库没有太大的区别，甚至还不如中心化数据库的效率高。事实上，中心化和去中心化永远是相对的，私有链可以看作一个小范围系统内部的公有链，如果从系统外部来观察，可能觉得这个系统还是中心化的，但是以系统内部每个节点的眼光来看，当中每个节点的权利都是去中心化的。

私有链和公有链另外一个巨大的区别就是，一般公有链肯定在内部会有某种代币，而私有链却是可以选择没有代币的设计方案。对于公有链而言，如果要让每个节点参与竞争记账，必定要设计一种奖励制度，鼓励那些遵守规则参与记账的节点，而这种奖励往往就是依靠代币系统来实现的。但是对于私有链来说，节点基本上都是属于某个机构内部的，这些节点参与记账本身可能就是该组织或机构上级的要求，记账对于它们而言就是工作的一部分，因此并不是一定需要通过代币奖励机制来激励每个节点进行记账的。所以可以发现，代币系统并不是每个区块链必然需要的。考虑到处理速度及账本访问的私密性和安全性，私有链可能更适合商业应用，越来越多的企业在选择区块链方案时，也会更多地倾向于选择私有链技术。

私有链具有如下特点。

（1）交易速度非常快。一个私有链的交易速度可以比任何其他类型的区块链都快，甚至接近于并不是一个区块链的常规数据库的速度。这是因为就算少量的节点也都具有很高的信任度，并不需要每个节点来验证一个交易。

（2）更好地保障隐私。私有链使得在那个区块链上的数据隐私政策像在另一个数据库中似的，不用处理访问权限和使用所有的老办法，但这个数据不会公开地被拥有网络连接的任何人获得。

（3）交易成本大幅降低，甚至在零私有链上可以进行完全免费或非常廉价的交易。如果一个实体机构控制和处理所有的交易，那么它们就不再需要为工作收取费用。即使交易的处理是由多个实体机构完成的，如竞争性银行，由于它们可以快速地处理交易，所以费用仍然是非常低廉的。这并不需要节点之间的完全协议，所以很少的节点需要为一个交易而工作。

（4）有助于保护其基本的产品不被破坏。正是这一点使得银行等金融机构能在目前的环境中欣然接受私有链，银行和政府在看管他们的产品上拥有既得利益，用于跨国贸易的国家法定货币仍然是有价值的。

【课堂训练 1-6】请简要说明区块链的三种类型。

任务实施

1.2.2 超级账本应用

1. 超级账本简介

超级账本（Hyperledger）是当前最著名的联盟链基础平台，是由 Linux 基金会于 2015 年发起的推进区块链数字技术和交易验证的开源项目，含 30 家初始企业成员（包括 IBM、Accenture、Intel、J.P.Morgan、R3、DAH、DTCC、FUJITSU、HITACHI、SWIFT、Cisco 等）。超级账本的目标是让成员共同合作，共建开放平台，满足来自多个不同行业的各种用户案例，并简化业务流程。

由于点对点网络的特性，分布式账本技术是完全共享、透明和去中心化的，故非常适合于金融行业，以及制造、银行、保险、物联网等其他行业中的应用。通过创建分布式账本的公开标准，实现虚拟和数字形式的价值交换，如资产合约、能源交易、结婚证书，能够安全、高效、低成本地进行追踪和交易。

2. 超级账本的组成

作为一个联合项目，超级账本由面向不同目的和场景的子项目构成，目前包括 Fabric、Sawtooth、Iroha、Blockchain Explorer、Cello、Indy、Composer、Burrow 等 8 大顶级项目，所有项目都遵守 Apache v2 许可。

3. 超级账本架构设计

超级账本包括三大组件：区块链（Blockchain）、链码（Chaincode）、成员权限管理（Membership）。超级账本的典型架构如图 1-1 所示。

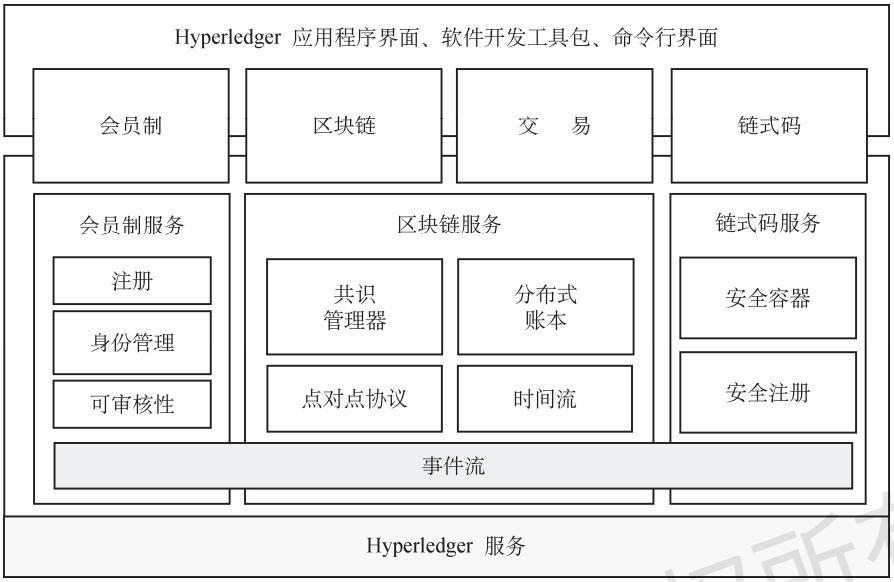


图 1-1　Hyperledger 典型架构

区块链提供了一个分布式账本平台。一般情况下，多个交易被打包进区块中，多个区块构成一条区块链。区块链代表的是账本状态机发生变更的历史过程。

链码包含所有的处理逻辑，并对外提供接口，外部通过调用链码接口来改变世界观。世界观是一个键值数据库，用于存放链码执行过程中涉及的状态变量。

成员权限管理基于 PKI，平台可以对接入的节点和客户端的能力进行限制。

4. 超级账本应用场景

超级账本主要应用于开放可信供应链、资产存管、商务合同、银联积分交换平台、商品身份溯源、食品安全等。

任务评价

填写任务评价表，如表 1-2 所示。

表 1-2　任务评价表

工作任务清单	完成情况
学习区块链分类	
学习联盟链技术解决方案（超级账本）	

任务拓展

【拓展训练 1-2】你认为哪些行业适合使用联盟链？请举出 5 个使用联盟链的行业示例。

任务 1.3　区块链应用

任务情景

【任务场景】

近年来，区块链作为一种新兴的应用模式被不同行业广泛使用。在金融、物联网、社会公益、供应链等领域中，出现了很多应用落地的探索和尝试。其中，供应链领域由于市场规模大、多信任主体、多方协作等特点，成为备受瞩目的区块链技术“用武之地”。那么，区块链在供应链金融场景中是如何被应用的呢？

【任务布置】

（1）学习区块链应用价值。
（2）学习区块链应用场景。
（3）理解区块链在供应链金融场景中的应用。

知识准备

1.3.1　区块链应用价值

区块链提供一种在不可信环境中进行信息与价值传递的交换机制，是构建未来价值互联网的基石，也符合党的十九大以来一直提倡的区块链要为实体经济提供可信平台。区块链发展到现在，我们可以从以下几个方面来分析其应用的方向。

（1）从应用需求视角来看，区块链行业应用正加速推进。金融、医疗、数据存证/交易、物联网设备身份认证、供应链等领域都可以看到区块链的应用。娱乐、创意、文旅、软件开发等领域也有区块链的尝试。

（2）从市场应用来看，区块链正逐步成为市场的一种工具，主要作用是减少中间环节，让传统的或高成本的中间机构成为过去，进而降低流通成本。企业应用是区块链的主战场，具有安全准入控制机制的联盟链和私有链将成为主趋势。区块链也将促进公司现有业务模式重心的转移，有望加速公司的发展。同时，新型分布式协作公司也能以更快的方式融入商业体系。

（3）从底层技术来看，区块链有望推进数据记录、数据传播和数据存储管理模式的转型。区块链本身更像一种互联网底层的开源协议，在不远的将来会触动甚至取代现有的互联网底层的基础协议（建筑在现有互联网底层之上，作为一个新的中间层，提供可信的、有宿主的、有价值的数据）。把信任机制加到这种协议里，将会是一个重大的创新。在区块链应用安全方面，区块链安全问题日渐凸显，安全防卫需要从技术和管理两方面全局考虑，安全可信是区块链的核心要求，标准规范性日显重要。

（4）从服务提供形式来看，云的开放性和云资源的易获得性决定了公有云平台是当前区块链创新的最佳载体，利用云平台让基于区块链的应用快速进入市场，获得先发优势。区块链与云计算的结合越发紧密，就越有望成为公共信用的基础设施。

（5）从社会结构来看，区块链技术有望将法律、经济、信息系统融为一体，颠覆原有社会的监管和治理模式，组织形态也会因此发生一定的变化。虽然区块链技术与监管存在冲突，但矛盾有望得到进一步调和，最终会成为引领人们走向基于合约的法治社会的工具之一。什么领域适合区块链技术？我们认为在现阶段适合的场景有三个特征：第一，存在去中心化、多方参与和写入数据的需求；第二，对数据真实性要求高；第三，存在初始情况下相互不信任的多个参与者建立分布式信任的需求。

区块链应用的发展趋势如图 1-2 所示，从比特币加密数字货币到金融结算市场的优化，逐渐演进到创造性地重构传统行业的大量应用，如供应链金融、供应链溯源、新能源交易系统、物联网等。随着应用场景日益丰富，应用将推动着区块链技术不断完善，区块链与云的结合日趋紧密，该技术也会逐渐应用于新兴市场经济，如房屋租赁共享经济、社交网络、内容分发网络等场景中。区块链系统以其特有的价值实现数据流转过程中的不可逆，从而保障数据的可靠性；区块链数据流转的可信性将有效简化流程、提升效率、降低成本；区块链的系统架构和优势使构建产业生态更加容易，并降低产业成本。可以预见，区块链是价值网络的基础，将逐渐成为未来互联网不可或缺的一部分，区块链技术也将逐步适应监管政策要求，逐步成为科技监管领域的重要组成部分。

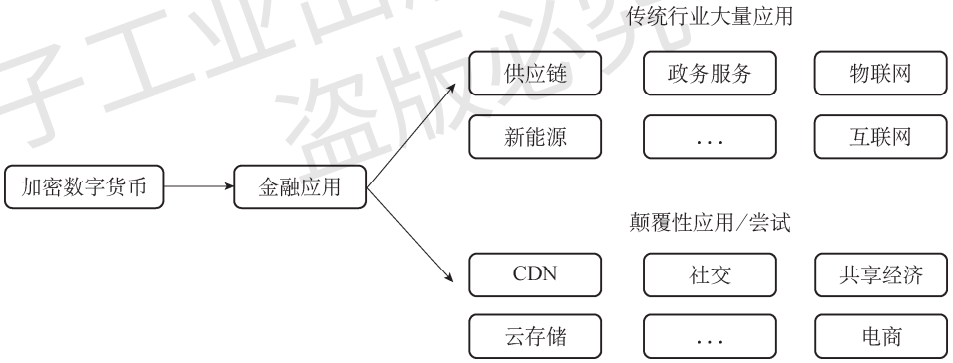


图 1-2　区块链应用的发展趋势

【课堂训练 1-7】请简述区块链应用的价值。

1.3.2　区块链应用场景

1. 区块链在教育领域的应用

教育是国之大计、党之大计。党的二十大报告中首次将“实施科教兴国战略，强化现代化建设人才支撑”作为一个单独部分，充分体现了教育的基础性、战略性地位和作用，并对“加快建设教育强国、科技强国、人才强国”做出全面而系统的部署，为到 2035 年建成教育强国指明了新的前进方向。

目前，教育领域主要有以下一些方向可以利用区块链技术进行改善。

首先是各类证书作假与学术欺诈问题。伊利诺伊大学物理学教授 George Gollin 对文凭

造假现象进行调查后发现，仅美国每年就有约 20 万份虚假学历证书从非法文凭提供商处售出。造成学术欺诈的一个重要原因就是教育信息统计的不完整和分散，使得认证成本高，验证困难。其次，简历等个人经历信息不对称。企业为了验证简历上所有信息真实无误要付出的成本极高，何况部分信息如实习经历、工作经历等并未进行数字化的录入，难以进行查验，这给应聘者在简历造假上创造了可能，招聘时的人才资历真实性认证存在难点。第三，当前在线教育的教学质量无法保证。由于在线教育的信息不对称性强，教育机构与教师的资质、教育评价都可能存在造假的情况，学生及家长难以判断教育机构的服务质量。

因此，对于以上信息不对称的情况，区块链技术可以利用其不可篡改、可追溯的特点来保证教育信息的真实性。

对于学生个人建立全维度的教育和职业信息体系。除了将学历学位及学习成绩等常规的学生信息上链储存，同时也能记录学生在学习过程中的其他重要数据，如课堂出勤率、奖项荣誉、社团活动、实习经历、职业等级证书等。在求职过程中，通过建立企业、学校的互通，让企业将学生或员工的实习经历、工作经历上链，使得企业招聘时能够直接从区块链平台上获得相关的真实数据。链上数据的真实性让企业无须再花费大量人力及成本对应聘者进行背景调查。

对于教师建立链上评价体系和教师个人价值体系。学生或家长可以在接受教育服务后对教育机构或教师的服务进行真实评价并上链，这些评价会倒逼教育服务提供者提升自身的教学质量，杜绝虚假教学资质的教育机构及教师的存在，保障学生的权益。另一方面，对于有出色教学内容和评价的教师可以建立自己的链上价值，跳出中介平台直接和学生进行点对点的教育和知识付费活动。

案例分析

广西壮族自治区高等教育自学考试网络助学平台“正保自考365”

“正保自考 365”是正保远程教育旗下以自考咨询和自考辅导课程为主的教育型网站，拥有由 2000 多名老师及 300 多名高校教授组成的强大师资团队，以及完整的教学体系。“正保自考 365”也是广西招生考试院唯一指定的网络助学平台。目前广西壮族自治区的广西大学、广西民族大学、广西师范大学、桂林电子科技大学等众多院校均已加入该平台，且已有 70 个国家及地区承认该网站颁发的高等教育自学考试学历及学位。

由于“正保自考 365”是一个在线教育网站，学生的过程性考核、课程表现等较为细节的学习过程无法被很好地监督和认证，对于学生的学习激励作用也不够强。而区块链技术拥有不可篡改、可验证等特点，可以基于区块链记录存储学生的学习过程，对其学习行为进行细致的追踪和记录。这一方面有利于学校更好地管理学生学习状态，提供更具个性化的培养计划；另一方面也可以为学生颁发区块链上的学习证明，更具有可信度，促进学生、教育机构和企业共享学习过程和学习认证等方面的数据，建设可信的教育信息化管理平台。

因此，为确保考核成绩及学历学位真实可信，正保远程教育将区块链技术引入自考平台内，利用区块链技术对自考学生的培训过程、考核成绩、学历学位等信息进行认证记录，促进学生、教育机构及企业之间的数据共享，打破当前数据孤岛的现状，让数据更加透明。同时，正保远程教育利用区块链点对点传输、可验证、不可篡改及可追溯等

特点，对学生的教育背景提供可靠的数据支撑，并且做到数据的可信、可追溯，便于毕业审核及招聘单位寻求人才。

正保远程教育的区块链平台“Link100 职业能力链”已经于 2019 年 3 月获得国家互联网信息办公室发布的第一批境内区块链信息服务备案。正保自考平台也给自考生颁发了国内首批“区块链结课证书”。如图 1-3 所示的是“正保自考 365”的一份链上结课证书。

图 1-3　“正保自考 365”链上结课证书

2. 区块链在医疗领域的应用

医疗健康行业以保障人民群众身心健康为目标，主要包括医疗服务、健康管理、医疗保险及其他相关服务，涉及的产业面广、产业链长，包括制药制剂、医疗器械、保健用品、保健食品及健身用品等。

随着互联网科技的发展，传统医疗产业的信息化、数字化改造已大部分完成，“互联网+医疗”的各种商业模式也趋于成熟，进入了稳健发展阶段。寻医问诊、报销支付等流程变得更加便捷和扁平化，互联网技术的嵌入也解决了部分信息不对称的问题，但由于医疗领域的特殊性，行业当前仍存在许多问题或症结尚未解决。

其中最主要的问题来自医疗数据的隐私敏感性造成的数据孤岛。相关法律规定，医疗机构应当将患者的数据严格保密保存，因此多数医疗机构不轻易、也不能将医疗信息对外公开，这造成医疗信息流通不顺畅，各个医疗机构形成了数据孤岛。这就导致了就医过程中诸多的不便，如在患者转院转诊的过程中，患者将面临相同项目重复检查的窘境，造成金钱及时间上的浪费，医疗资源未能有效利用，患者就医体验差。数据孤岛也导致临床数据缺失，不利于药物研发。

此外，在药品方面，由于缺乏适当的追踪机制，药物供应链中从制造、流通、贮藏到销售等环节存在着部分的不规范现象，难以根除假药、劣药的制造销售，如医药销售网点

不具备经营资格、药物或疫苗贮藏标准不达标等。

使用区块链技术，将在保障患者数据隐私的前提下，打通医疗数据的信息流通，改善医疗机构之间互为数据孤岛的现状，重建医患之间的信任，提高行业效率。

在医疗诊断中，使用区块链技术构建电子病历数据库，将患者的健康状况、家族病史、用药历史等信息记录在区块链上，并结合 MPC（安全多方计算）、TEE（可信执行环境）等隐私保护技术保护患者相关信息数据，确保患者隐私不被侵犯。通过区块链平台上的数据共享，更大范围的、不同层次的医疗机构之间的信息通道得以打通，并可以设置数据使用权限。这样，将减少患者的重复诊断，提高就医体验感。数据孤岛打通后，临床医疗资料也可以被更好地利用，有助于进行后续研发。

针对假药、劣药，可以建立基于区块链的药物供应链平台，本质上是商品的溯源。从药物原材料的获取到药物的生产制作、贮藏和流通销售等环节，进行适当的监控和追踪。消费者可以通过区块链平台看到所购买药品的生产厂家、日期数据及流通环节等是否符合标准，也可通过区块链技术配合物联网对药物或疫苗的贮藏温度、出入库时间等进行实时监控，保证药物的真实性与质量安全，在原本《药品经营质量管理规范》（GSP）及《药品生产质量管理规范》（GMP）的强有力监管的基础上，进一步实现公开监管与追踪，打击假药、劣药市场，保障各方权益。

案例分析

阿里健康常州市“医联体+区块链”项目

2017 年 8 月 17 日，阿里健康宣布与常州市开展“医联体+区块链”试点项目的合作，将区块链技术应用于常州市医联体底层技术架构体系中，期望解决长期困扰医疗机构的信息孤岛和数据隐私安全问题。

该方案目前已经在常州武进医院和郑陆镇卫生院实施落地，将逐步推进到常州天宁区医联体内所有三级医院和基层医院，部署完善的医疗信息网络。

阿里健康在该区块链项目中设置了多道数据的安全屏障。首先，区块链内的数据均经加密处理，即便数据泄露或被盗取也无法解密。其次，约定了常州医联体内上下级医院和政府管理部门的访问和操作权限。最后，审计单位利用区块链防篡改、可追溯的技术特性，可以全方位了解医疗敏感数据的流转情况。

引入阿里健康的区块链技术后，在医联体内实现医疗数据互信互通，优化了医生和患者的体验，同时也推进了分级诊疗、双向转诊的落实。通过区块链网络，社区居民能够拥有健康数据所有权，并且通过授权实现数据在社区与医院之间的流转；医联体内各级医院医生可以在被授权的情况下取得患者的医疗信息，了解患者的过往病史及相关信息；患者无须做重复性的检查，减少为此付出的金钱及时间。如图 1-4 所示为常州医联体区块链应用流程示意图。

区块链技术实现了医院之间的信息互信互通，符合政府“让数据多走路，人只走一次路”的指导方针，但这样的技术应用会减少患者检查次数，相应减少医院的收入，以及降低人事费用，可能会触犯到相关方的利益。因此，这样的技术应用需要政府带头试点，自上而下地推行，并且需要推出新的商业模式，激励其他医院加入该生态中，生态整体才能健康可持续地运行。

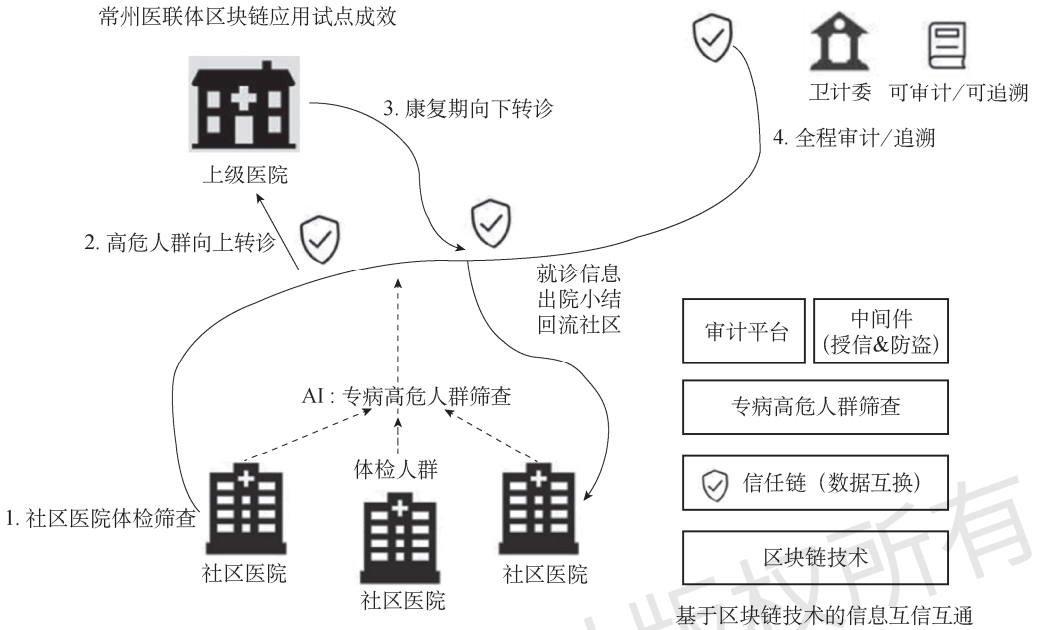


图 1-4　常州医联体区块链应用流程示意图

3. 区块链在公益方面的应用

公益事业包括慈善捐助、志愿服务、公益扶贫等领域。近些年，受到一些负面案例的影响，慈善行业的受信任程度实际上在不断被削弱。目前，公益捐助等领域存在资金和物资流向不透明、使用率不高，社会监督与公开机制不够健全等问题。不少现行的公益慈善机构采用的机制不够透明。它们往往会搭建多个资金池，众多捐助者向资金池中注入善款，同时管理单位再通过资金池向需要扶贫支持和公益支持的个人和团体提供资助。很多时候慈善机构的行为都是黑盒，捐助人无法真正了解资金和物资的去向，导致可能有作恶者从中渔利，从而影响大众的公益热情。另外，公益活动中还存在资金利用效率低的问题，这源于信息的分割和应急机制的不健全。

区块链可以在公益领域发挥它的特点，优化慈善流程，建设可信体系，增进公众对第三方慈善机构的信任和信心。

其一，提高资金和物资流向透明度。慈善机构、捐助者、受捐者、上下游环节、三方监督等相关机构和个人，可以成为区块链系统节点，对相关款项进行链上实时核验和跟踪。一方上链后，其他多方共同监督。当捐助者、三方监督机构或受捐者发现资金数量不对，那么可以对中间环节进行质询和复核，这样将会大大提高问题的发现和解决效率。同时，利用区块链公开透明的特点，也可以让所有捐赠明细上链，接受公众监督。

目前某些慈善机构通过数字资产接受捐助，例如 2019 年 10 月，联合国儿童基金会（UNICEF）宣布设立加密数字货币基金，接受比特币等加密数字资产的捐助。数字资产由于是区块链原生资产，可以确保捐款资金的真实性，可以实时了解捐赠资金走向，简化捐助人的捐款流程，使捐助更方便快捷，尤其在跨地区、跨境捐助上提高了效率，降低了成本。

其二，建设基于区块链的公益信息共享平台，提高资金管理和利用程度。通过区块链系统，可以共享各慈善机构需要救助和捐款的信息，使捐助者更全面地了解需求信息，使机构能综合利用资金和物资，确保分配给最紧急、效用最高的需求者。同时，管理机构也可以接入区块链，进行实时监督、指挥、调配，做好全局工作，进一步提高资金和物资的利用程度和管理效率。

案例分析

支付宝区块链爱心捐赠追踪平台

传统的捐款平台由运营方发布募捐信息，捐款者将款项交予运营方，再由运营方将款项拨送至募捐方。而运营方对款项使用情况公布不透明，难以获得公益参与者的信任。当更多人参与公益时，如何确保善款能够被精准地送到受捐者手里就成了公益的焦点，捐赠款项去向透明化成为公益事业的重中之重。

因此，蚂蚁金服应用区块链，与中华社会救助基金会合作，在支付宝爱心捐赠平台上线了“听障儿童重获新声”公益项目。这个项目是区块链在公益场景运用中的一次尝试，所募集善款将用于十名听障儿童的康复，筹集目标为 198 400 元。此项目相比于传统公益，最大的不同之处在于可以追踪善款流向。

支付宝上的善款来源非常分散，作为小型筹款项目，每次所接受的捐赠数额较小。因此，这样一个项目接受了超过万次的捐赠。由于区块链的分布式记账，每次捐赠都会将捐赠金额、捐赠时间、捐赠人等信息记录在区块链上；每笔善款流向也以同样的方式记录。区块链具有不可篡改性和可溯源性，任何用户都可以随时查询公益项目筹款进度与款项用途，使公益事业能够实现公开透明，能够赢得公众的信任。

4. 区块链在政务领域的应用

近年来，“互联网+政务”快速发展，国家机关在政务活动中，全面应用现代信息技术、网络技术及办公自动化技术等多项技术进行办公、管理和为社会提供公共服务，也称为电子政务。

我国电子政务概念的雏形产生于 20 世纪 80 年代，在 1999 年开始得到重视并开始逐步建设电子政务平台，推进政府工作的自动化、信息化。2018 年 10 月，西藏自治区政务服务网开始试运行，标志着我国 32 个省级网上政务服务平台体系已基本建成。截至 2018 年 12 月，我国共有政府网站 2 817 962 个，主要包括政府门户网站和部门网站。

虽然说我国在电子政务发展上已属于较为领先的国家，但在数据交互、协同、共享上仍面临诸多困难。

（1）跨部门协作与数据共享不足。“互联网+政务”的发展，使得电子政务服务实现了相当大的飞跃，企业、群众可以通过网上服务入口办理多项业务。早期电子政务系统均是根据不同部门自身业务需求独自搭建的，各部门独自构建了一套互联网政务体系，致使各部门之间的网络基础设施、业务系统、数据资源处于割裂、碎片化状态，并且缺乏标准统一的数据结构和数据接口，导致同地区的政务系统跨部门数据共享和业务协同力度不足。从现有情况来看，企业、群众网上办事需要登录不同部门的网站，各部门没有形成高效的

政务服务协同机制，信息重复采集的情况较为普遍。

（2）城市数据监督不到位。现有的电子政务改革过程中，城市数据的治理与监督并未得到足够重视，政府监督与管控时而出现盲区，时而出现监管缺位。以城市治理为例，针对政府的重大投资项目、重点工程和社会公益服务等敏感领域，依靠信息公开并不能形成有效的约束力，在这些项目的进行过程中，政府实际上在某些情况下存在一定盲区，当出现违法违规操作时，并不能及时发现，造成监管缺位，一旦这些项目出现问题，将对政府公信力造成一定影响。另外，现有的政府信息管理框架并不能对城市数据进行有效采集、校核、加工和存证，一旦出现违法违规事件，证据的缺失对调查取证、追责等带来巨大困难。

区块链技术为跨地区、跨部门和跨层级的数据交换和信息共享提供了可能，提供了可追溯、可监管的政务信息。区块链助力跨部门政务协作示意图如图 1-5 所示。

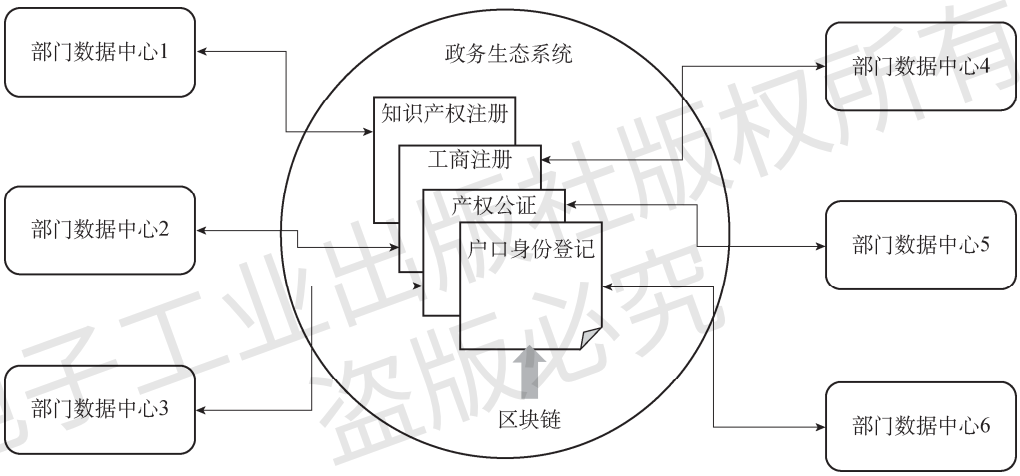


图 1-5　区块链助力跨部门政务协作示意图

首先，区块链的分布式数据结构有利于建立政府部门之间的信任和共识，在确保数据安全的同时促进政府数据跨界共享。所有部门都可以成为链上节点参与“记账”，且数据公开透明，数据的交换都有迹可循，数据交换的容错率也较高，这就为建立和维系政府部门之间的信任和共识提供了技术条件。即便是层级和规模都很小的政府部门，也可以通过区块链技术参与数据共享。这就大大提升了政务服务的整合力度，真正实现“数据跑路”取代“人跑腿”，提升群众的获得感和满意度。

同时，区块链应用有利于明确政务数据归属权，明晰数据权责界定。结合公私钥体系，政务数据一经产生就确定了归属权与管理权，为后续的授权使用明晰了权责归属。另外，结合智能合约技术，能够实现数据共享与业务协同过程中的使用权的权限与分配。在政务数据授权共享、业务协同的同时，能够将所有的数据流转使用记录留存于链上，凭借区块链所具有的不可篡改、可溯源的特性，为后续数据泄露等事故提供有迹可循的、清晰的溯源依据。

区块链也能赋能城市数据监督，提升管控力与约束力。区块链能够发挥其数据的不可篡改特性，结合物联网技术，实现城市政务数据的全流程存证，扫清原本因技术局限

无法覆盖的监督盲区，补足监管的缺位，增强城市数据监督管控与约束力，为后期的核验、举证等提供便利，提升政府公信力。例如，在政府重大投资项目上，实现建设主体的全流程数据上链，利用区块链的存证和不可篡改特性，对其产生较大约束力。此外，通过将相关监管机构、企业纳入区块链生态中，通过数据上链，促使监管机构能够实现更全面的监管，营造良好的监管环境，并为未来利用数据进行科学决策、建立建全智慧政府提供坚实的支撑。

案例分析

江苏南京区块链电子证照共享平台

2017 年，南京市信息中心牵头，启动了如图 1-6 所示的南京市区块链电子证照共享平台的项目建设，将房产交易、人才落户、政务服务等多项民生事项纳入区块链政务数据共享平台中，实现了政务数据跨部门、跨区域共同维护和利用。南京市现在的政务数据和电子证照绝大多数通过区块链政务数据共享平台共享到各个业务系统，包括工商、税务、房产、婚姻、户籍等。

到 2019 年，南京市区块链电子证照共享平台已经对接公安、民政、国土、房产、人社等 49 个政府部门，完成了 1600 多个办件事项的连接与 600 多项电子证照的归集，涵盖全市 25 万企业、830 万自然人的信息。

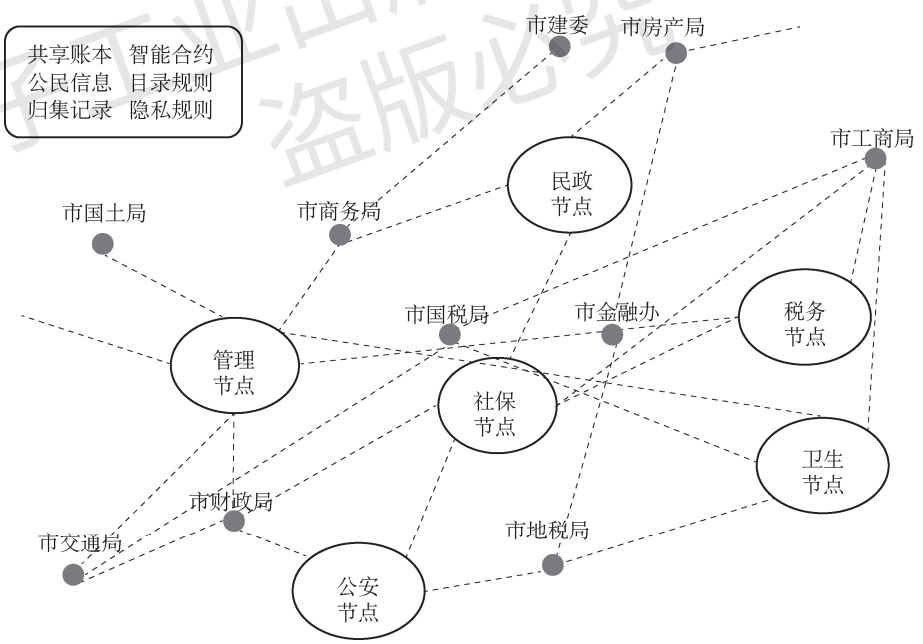


图 1-6 南京市区块链电子证照共享平台示意图

案例分析

区块链服务网络（BSN）——政务专网

区块链服务网络是由国家信息中心领导，由中国移动通信集团公司、中国银联股份有

限公司、北京红枣科技有限公司主导的首个国家级联盟链。其致力于打造跨公网、跨地域、跨机构的区块链服务基础设施，推出了针对政务的专网产品——区块链政务专网（BSN）。BSN 以联盟链为基础架构，通过公共城市节点建立连接，形成区块链全球性基础设施网络。BSN 公网类似于互联网，BSN 专网则类似于局域网，专网依托于公网的技术架构，可以实现与公网的互联互通。

在技术架构的设计上，BSN 政务专网的基础设施层支持专有网络、公有云、私有云等部署形态，也支持跨网混合部署；区块链平台层则支持 Hyperledger Fabirc，Fisco BCOS 等区块链引擎；节点网关层则提供封装的、通用的、稳定的、可靠的服务和接口。

在实际应用上，政务专网将为各系统、各部门、各用户分配统一的身份 ID，实现数据与应用的统一管理，运营平台也将针对区块链应用的接入采用统一审核制度，确保应用的安全准入机制；区块链政务专网内提供多种通用的内置应用，能够实现各系统数据的融合共享、公文档案的安全存储及电子合同签章等功能；各委办局在接入系统后，可以将自己的业务需求共享到平台上，并且由委办局自行定义数据结构与进行脱敏操作，数据上链后，使用单位将在原数据归属者的授权下获取数据，提升数据共享效率与实现数据协同。

在安全架构设计上，全方位考虑了包括身份鉴别、访问控制、安全审计、通信保密、资源控制、主机安全等十个方面。如图 1-7 所示展示了 BSN 政务专网架构。

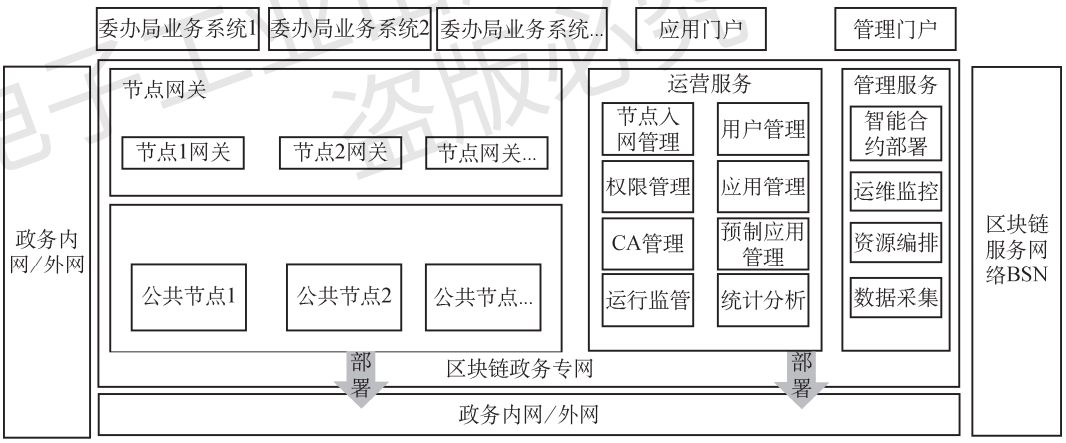


图 1-7　BSN 政务专网架构

BSN 政务专网已经在杭州城市大脑平台成功部署，且在一周时间内就完成了“城管道路信息及贡献管理”“酒店消毒管理”“内部最多跑一次”等多个应用的上链，产生了良好的效果。

2020 年，依托区块链技术，杭州市下城区创造性地搭建了“1Call 链”项目，使疫情大数据实现了全网同步、安全加密，极大提高了数据获得率和安全性。

据下城区数据资源管理局相关负责人介绍，员工在线填写承诺书并提交后，会自动生成一个“承诺书特征码”同步到区块链，确保电子承诺书相关数据不被修改。不仅员工自己可以进行单击查询，后台也可以通过特征码对不同员工的承诺书进行分类鉴别保存，确

保信息的安全、透明、有效，提高办事效率。

与此同时，后台信息的分类鉴别也为线下工作提供了参考。通过杭州城市大脑平台“工地复工精密智控管理系统”，工作人员可以统计出未来 3～7 天内即将返杭员工的来源地、所属项目，合理安排包车。

5. 区块链在智慧交通方面的应用

21 世纪以来，各国政府积极助推现代化交通体系建设，尤其重视交通运输智能化与信息化建设。智慧交通、数字化信息的发展成功赋能集约化交通体系的构建，成为解决现代交通痛点的核心方向。信息化、网络化、智能化的交通运输系统建设能有力推动国家交通体系的跨越式发展，并进一步缓解资源与环境压力。

对于交通运输行业，区块链主要在以下方面进行赋能。

（1）车辆认证管理。可以将车辆信息、车主信息等加密后上链，建立属于车辆的区块链身份标识，并与交通运输部门、车险公司等进行信息打通，可以更高效地进行信息互通，对车辆进行管理，进行违章等行为罚款的支付。

（2）助力智慧交通运输网络的优化。在智慧交通中引入区块链技术，并串联交通运输领域中的政府、企业等各行业主体，协助记录车辆、道路、桥梁、车站等基础设施实时情况。相比传统的交通运输信息网络，基于区块链的网络可以更好地在保护隐私的同时进行交通数据的互通，这有助于建设真实可靠的交通运输信息系统，进而提升智能交通的社会运行效率。

（3）汽车碳排放上链推动节能减排。在传统碳排放记录系统中引入区块链技术，有利于解决汽车行业既有的数据问题与认证问题。通过记录轿车、大型客车等车辆的驾驶与碳排放信息并整合上链，可以将碳排放追溯到个体角色，从而对驾驶员与相关企业做出评估，推动其进行节能减排。

案例分析

北京首汽建设新型区块链联动平台“GoFun”

2015 年 8 月，北京首汽集团成立 GoFun 平台，这是首汽为拓展移动出行业务建立的一款共享汽车产品，于 2016 年 2 月 25 日正式上线运营。目前，其业务主要由 B 端和 C 端两部分组成。

在 B 端，该联动平台利用以太坊开源架构搭建了一条联盟链 GFChain，将每台汽车的信息上链，致力于形成完备的车联网数据系统，推动车辆数据公开透明化。GoFun 还构建了与北京环交所的合作关系，积极推动汽车尾气排放量等基础数据上链，推动节能减排。

在 C 端，GoFun 针对用户租车中的闲置时间，提出了相应解决方案：当租车用户有 8 小时无须使用共享汽车时，可通过区块链信用机制，分享空余时间给其他用户，增强了同一时间段内，共享汽车的使用效率和频次。此外，GoFun 将用户的开车时间等行为转化为“能量方块”，激励租车用户多用多得，如用户可通过完成租用车辆、每日签到、邀请新好友等任务获得不等数量的“能量”，积攒到一定程度的能量可用于兑换租车优

惠券或其他礼品。除此以外，不同的车型、行驶里程、使用时间均会对用户挖到的“能量”的大小造成影响，挖取“能量”的能力也可通过完成实名认证、驾驶证认证、支付押金等多种方式提高。这增加了用户租用共享汽车过程中的趣味性，改善了平台用户的体验。

数据显示，2019 年 4 月，GFChain 实现超过 180 万的区块数，平均每区块完成 55 笔交易。“能量方块”特色业务的上线大大提升了用户留存率，平均每位用户为其额外停留 2 分钟。截至 2019 年年底，GoFun 出行已覆盖国内 84 个城市，拥有近千万注册用户，每辆车日均单量在 7 单以上，月度活跃用户达到 170 万人次，最高日度活跃用户直逼 75 万人次。

6. 区块链在智慧能源方面的应用

能源行业主要涉及电力、石油、天然气和新兴能源等领域，囊括上游的开采、勘探、生产，中游的提炼、分发、输送，以及下游的分销、交付和使用等。它是服务工业商业、居民生活的核心行业，维护着我们经济生活的正常运转。

进入 21 世纪以来，人类活动加剧，世界人口和总体经济产出大幅增长，同时也伴随着能源的大幅消耗。波士顿大学学者研究发现，即使气候维持当前变化，到 2050 年，全球能源需求还会上涨 25%。巨量的能源需求带来了气候变暖等问题，发展和使用清洁能源是所有人类应该重视的课题。

除此之外，贫富发展不均衡也是困扰能源行业的问题之一。在发达地区和欠发达地区会分别存在能源过度消费和能源不足的现象，如何促使能源均衡分配，是能源行业需要解决的问题。同样，平衡各发电站和用电者之间的关系，提高能源使用效率也是需要解决的问题。

区块链技术能够保证系统透明、稳定可信及防篡改，并且在点对点网络中存在可以自动执行的智能合约，这给能源行业带来了新的发展思路。

（1）能源供应链。能源市场交易的参与者众多，包括券商、交易所、物流公司、银行、监管机构和代理机构等。在传统的模式下，交易输送过程速度慢、耗时长，造成的摩擦成本将小型机构排除在外。如果应用区块链技术，上下游之间可以快速完成配合，交易时间和信息被记录在账本中，同时智能合约可以保证交易在特定的时间内执行，大大提高协作效率，节约纸质办公成本。

（2）分布式微电网交易，推动清洁能源发展。微电网是指由分布式电源、储能装置、能量转换装置、负荷、监控和保护装置等组成的小型发配电系统，实现分布式电源的灵活、高效应用，解决数量庞大、形式多样的分布式电源并网问题。开发和延伸微电网能够充分促进分布式电源与可再生能源的大规模接入，实现对负荷多种能源形式的高可靠供给，是实现主动式配电网的一种有效方式。而区块链是有效的微电网交易基础技术，可以让分布式的清洁能源（如太阳能）直接进行点对点交易，降低接入统一电网的成本，有效提高能源电力的利用率。同时微电网系统能够推进地区能源的产出和使用，减少能源运输的消耗，解决能源分布不均衡等问题，更有弹性和更高效。

案例分析

L03 Energy 成立布鲁克林微电网——TransActive Grid

2016 年 3 月 3 日，L03 Energy 与区块链技术创业公司 Consensys 合作成立 TransActive Grid 项目，在纽约布鲁克林开展新型微电网试验，这是区块链在能源领域的首次应用。

起初，TransActive Grid 项目只涉及十个分布在布鲁克林地区总统大道两侧的家庭。道路一侧的五户家庭安装了屋顶光伏发电系统，产生的电能在完全满足家庭用电需求之余，还有大量剩余；另一侧的五户家庭没有安装发电系统，因此需向对面家庭购买电力。据此，这十个家庭构成了一个微型的电力生态。因此，即便没有第三方电力运营商，家庭之间也可以通过区块链网络，采用 P2P 模式直接进行点对点的能源交易。如图 1-8 所示为 TransActive Grid 项目的系统设计。

智能电表作为这种电力交易模式的硬件基础，在底层应用了基于区块链的智能合约，可以采集包括发电能力、用电需求、交易电量等在内的用户信息。用户信息完成实时上链后，将同步至所有节点并分布式储存。系统不仅可以预测用电量从而智能化地应对能源需求，还能及时储存剩余能源并进行能源交易。

此外，区块链微电网还保证了即时交易的实现，消费者无须通过中间零售商便可进行能源批发的市场交易，随后使用智能设备实时自动地支付账单。当智能代理完成能源交易价格的分析后，将结合其预测出的特定用电需求，为客户形成更明智的消费策略：在能源价格低时，增加能源购买量，并储存多余能源于家庭储电设备；在能源价格上涨时，减少能源购买，甚至出售部分储存能源。

但是，目前该项目未实现大规模推广，主要原因是点对点交易的模式对于运营机构而言很难盈利。同时，纽约市也禁止个人直接参与电网市场。因此，考虑到对新能源发展的推动，此类项目更需要政府作为主要发起者进行建设和改革。

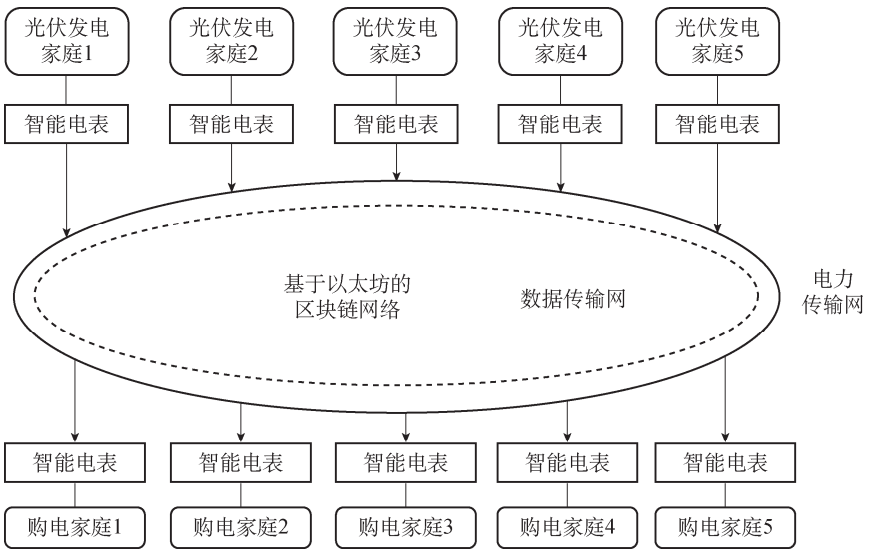


图 1-8　TransActive Grid 项目系统设计

【课堂训练 1-8】请简述几个区块链的应用场景。

任务实施

1.3.3　供应链金融业务应用实践

1. 供应链金融业务场景

供应链金融是贸易金融的一个典型场景，如图 1-9 所示，它是指在供应链的业务流程中，以核心企业为依托，运用自偿性贸易融资的方式，对上下游企业提供综合性金融产品和服务。整个行业在全球占据万亿级的市场。举个简单的例子来说明供应链金融业务，一家企业和供应商 A 签订采购合同，金额为 1000 万元，合同在 12 个月后到期，当然合同款也是在 12 个月后才能付清，然而供货的生产需要 600 万元的资金，传统金融思路是供应商不得不想办法去金融机构贷款并支付高额的利息，这就间接增加了生产成本，并且金融机构一方放款可能并不及时，放款金额也和该供应商的资质、信用甚至是抵押物有关。供应链金融就是试图使用新的方式来解决过程中各方的金融需求，如将业务过程中的采购合同作为抵押物，金融机构校验合同真实性后就可以和供应商 A 签订贷款合同，同时提前放款 600 万元给供应商，12 个月采购合同到期后，企业直接付 600 万元的本金和相应利息给金融机构，剩余的钱直接付给供应商 A，因此极大地降低银行的风险。

2. 行业现状

从上面的例子中可以看到这是一个三赢的局面，企业和供应商的业务可以正常开展，金融机构也能从中受益，所以供应链金融的核心思路就是打通传统供应链中的不通畅点，让业务流中的资金都可以顺利地流动起来。当然其中的过程有很多关键点，如合同是否真实、合同额有没有被非法篡改、企业有没有不诚信记录、合同到期后企业能否按时顺利地付款等。另外，在现行金融贸易领域中，存在高成本的人工核查、众多银行之间的信息不流通、监管难度大、中小企业申请银行融资的成本高等问题。银行在为客户办理业务时，通常通过人工的方式进行情报资料收集、信息对比验证、现场实地考察和监督，来了解客户情况和贸易背景，开展业务风险控制及管理。

3. 业务痛点

目前供应链金融的核心问题如图 1-10 所示。首先，高度依赖人工的交叉核查，即银行须花费大量时间和人工判定各种纸质贸易单据的真实性和准确性，且纸质贸易单据的传递或差错会延迟货物的转移及资金的收付，造成业务的高度不确定性。其次，金融贸易生态链涉及多个参与者，单个参与者只能获得部分交易信息、物流信息和资金流信息，信息透明度不高。再次，由于银行间信息互不联通，监管数据获取滞后，资金管理监管难度大，例如存在不法企业“钻空子”，以同一单据重复融资，或虚构交易背景和物权凭证。最后，中小微企业申请金融融资成本高。基于以上几个难点，为了保证贸易融资自偿性，银行往往要求企业缴纳保证金，或提供抵押、质押、担保等，从而提高了中小微企业的融资门槛，增加了融资成本。

综上可知，供应链金融的核心问题有三点：融资难、风控难、监管难。

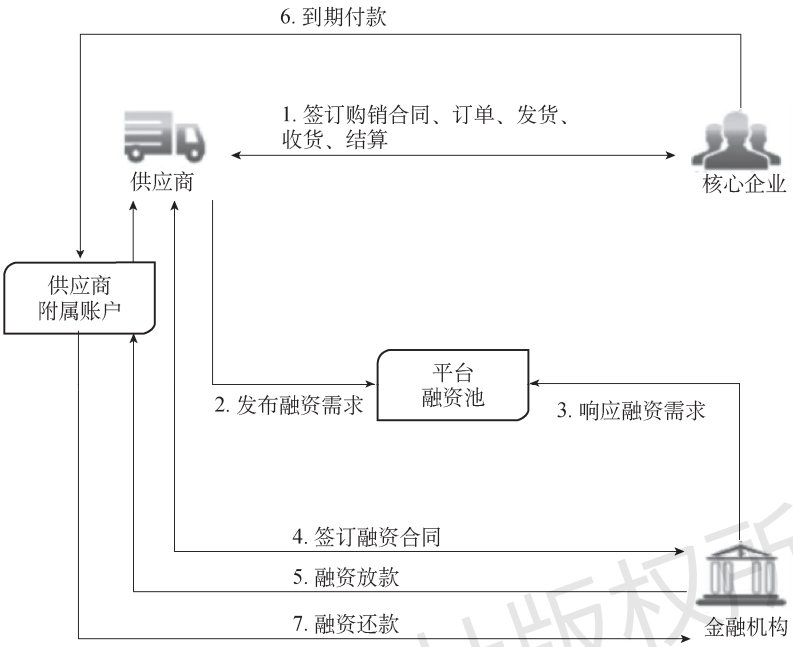


图 1-9　供应链金融场景

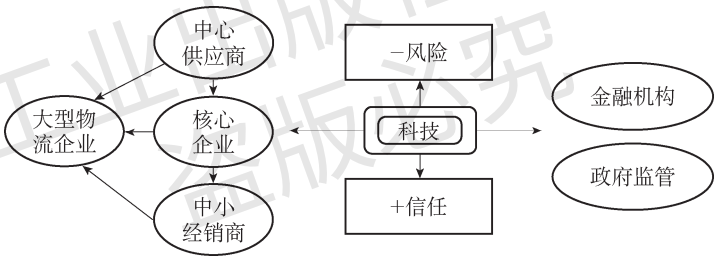


图 1-10　供应链金融核心问题

4. 基于区块链的解决方案

供应链金融场景中的关键需求是如何存证供应链的关键信息；如何确保可信资质的评估；如何保障交易各方的权益；如何建立供应链的上下游核心企业和供应商之间的互信，降低融资的成本。区块链技术提供的特性和这些需求高度吻合，不可篡改特性让数据很容易追溯，公私钥签名保证不可抵赖，这些机制可以让上下游企业建立互信，智能合约可以保障各方约定的合同可以自动执行。基于区块链可信机制的供应链金融解决了供应商单方面数据可信度低、核验成本高的问题，打通企业信贷信息壁垒，解决融资难题，提升供应链金融效率，通过供应链中各方协商好的智能合约，可以让业务流程自动执行，资金的流转更加透明，极大地提供公平性。

华为云 BCS 服务利用自身在供应链和区块链方面的业务和技术积累，携手合作伙伴，积极支持供应链金融结合区块链技术的创新，服务平台提供新型的智能合约引擎支持复杂的智能合约和高效的查询，提供创新共识算法支持峰值可达 10K TPS 的高性能并发交易，为该行业的进一步发展提供了良好支撑。基于区块链的供应链金融解决方案如图 1-11 所示，通过多级链结合起来，在每一级区块链中实现当前范围的可信数据共享，并基于授权，

按需把数据推送到下一级区块链系统中。基于共享账本及智能合约，不但解决了数据互信问题，同时提升了各方交易的效率。

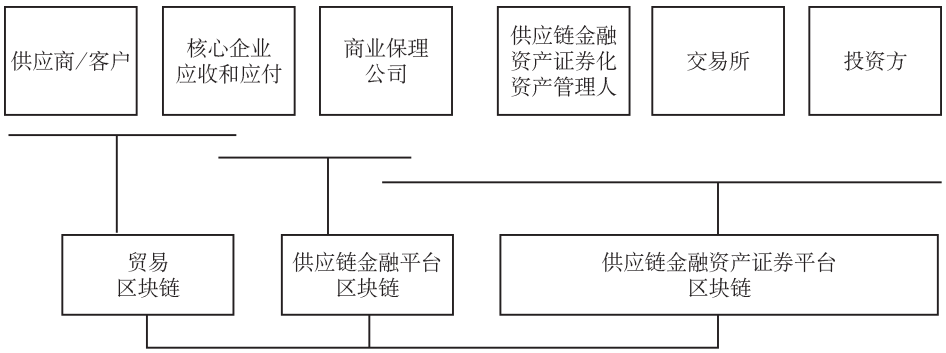


图 1-11　基于区块链的供应链金融解决方案

任务评价

填写任务评价表，如表 1-3 所示。

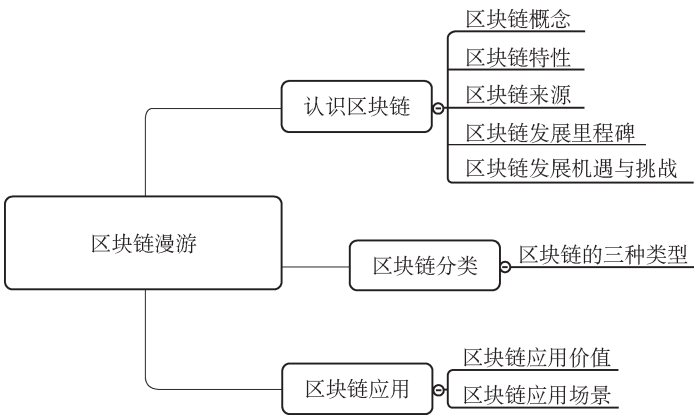
表 1-3　任务评价表

工作任务清单	完成情况
学习区块链应用价值	
学习区块链应用场景	
理解区块链在供应链金融场景中的应用	

任务拓展

【拓展训练 1-3】请举例说明区块链在实际生活场景中的应用。

归纳总结



测试习题

一、填空题

1. 大型云计算服务商在云的基础上提供区块链技术，优势在于_____、_____、_____三个方面。

2. 区块链的五大特点分别是_____、_____、_____、_____、_____。

3. 根据开放程度的不同，一般按照准入机制可将区块链分为_____、_____、_____。

二、单项选择题

1. 以下哪一个选项不属于区块链的特点？（　　）

A. 去中心化　　B. 不可篡改性

C. 完全封闭性　　D. 匿名性

2. 区块链凭借“不可篡改”“共识机制”和“去中心化”等特性，对物联网将产生的重要影响不包括（　　）。

A. 降低成本　　B. 提高设备寿命

C. 数据安全　　D. 追本溯源

3. 近年来，数字经济发展迅猛，数字经济成为多个国家发展经济的核心动能，在数字经济中，以下哪项技术不是推动数字经济的核心技术？（　　）

A. 人工智能　　B. 区块链

C. 大数据　　D. 化学化工

4. 2019 年 10 月 24 日，中共中央政治局第十八次集体学习中，习近平总书记在学习时强调要把哪项技术作为核心技术的自主创新突破口？（　　）

A. 云计算　　B. 区块链

C. 人工智能　　D. 人脸识别

5. 大数据、人工智能和区块链三者能否结合？（　　）

A. 不能结合，技术之间存在冲突

B. 没有必要结合，区块链技术可以代替大数据、人工智能

C. 没有必要结合，使用大数据和人工智能的场景，无须再使用区块链

D. 可以结合，有互相促进的关系，需要找到适合的结合方式

三、判断题

1. 大数据就是人工智能，人工智能就是大数据。（　　）

2. 区块链与人工智能主要是在底层技术方面，有诸多互补性。（　　）

技能训练

1. 分析区块链在实际场景中的应用。

2. 撰写联盟链技术解决方案实现报告。