

第3章 金融电子商务技术



【本章内容】

大数据技术

- 大数据概述
- 金融行业大数据现状
- 金融大数据发展展望

云计算技术

- 云计算概述
- 云计算应用与发展
- 金融行业云计算应用现状

区块链技术

- 区块链概述
- 区块链原理
- 区块链技术在金融领域的应用

人工智能技术

- 人工智能概述
- 人工智能的核心技术
- 人工智能的应用领域

移动互联网技术

- 移动互联网概述
- 移动互联网技术架构
- 移动互联网在金融领域的应用

物联网技术

- 物联网概述
- 物联网的关键技术
- 金融物联网发展情况



【学习目标】



知识目标

- ◇ 熟悉金融电子商务的前沿技术环境
- ◇ 理解大数据、云计算、区块链、人工智能技术
- ◇ 掌握移动互联网、物联网技术

能力目标



- ◇ 能够利用移动互联网技术从事金融电子商务业务
- ◇ 能够针对不同金融电子商务业务选择相应的前沿技术
- ◇ 学会使用物联网技术

**【案例导入】****AIC 人工智能币**

2016 年创立的万众金福(北京)科技有限公司是一家从事区块链技术与创新的 IT 公司,该公司经过长时间沉淀,在多位区块链领域专家共同努力下研发出全球第一款拥有人工智能技术与区块链技术双技术系统的数字货币——AIC 人工智能币(Artificial Intelligence Coin),并于 2017 第四届区块链国际峰会(2017 年 8 月 15 日在上海召开)上,面向全球发布。作为区块链应用的新秀,AIC 人工智能币受到业内外人士的密切关注。AIC 人工智能币旨在作为机器人与机器人之间的交易介质,以及机器人与人之间的交易介质。AI 便是人工智能的英文缩写,它是研究、开发用于模拟、延伸和扩展人的智能的理论、方法、技术及应用系统的一门新的技术科学。AIC 人工智能币的工作原理与大部分基于区块链的数字货币类似,其总体结构为去中心化的结构,其核心算法采用的是 Scrypt 算法,发行总量为 10 亿。目前,AIC 人工智能币不但有 PC 端的电脑钱包,还有手机端的冷钱包,而且参与官方众筹的种子用户全部都参与了官方的冻结锁仓计划,每月解冻 10%。今后一段时间,万众金福(北京)科技有限公司还会继续推出 AIC 人工智能交易、AIC 机器人社区、AICVR 社区、AIC 开放社区等。未来,AIC 人工智能币会应用于机器人、人工智能、VR 智能产品、多媒体产品、数码产品、虚拟现实世界等。

(资料来源:网易新闻,<http://news.163.com/17/0825/01/CSL95HF4000187VG.html>,2017-08-25)

金融电子商务的发展得益于金融科技的迅速发展。随着大数据、云计算、区块链、移动互联网、物联网等新一代信息技术的发展和应用,金融和科技正在不断融合。

金融科技能够有效地提高金融服务的可获得性和便捷性,降低金融交易成本。高科技产业和金融产业都是高风险、高回报的产业,金融产业又属于时效性和操作性强的产业,大量的新技术被应用于金融业,由此产生的新模式和高额的回报反过来又促进了相关技术的发展,这样的良性循环使得金融电子商务的发展大大加快。

3.1 大数据技术

在工业时代的经济发展范式中,劳动力、土地、资本都是重要的生产要素。而在信息时代,互联网和云计算已成为信息经济运行的基础设施,大数据也成为经济发展中越来越重要的新兴生产要素。

3.1.1 大数据概述

金融业是数据利用率极高的行业之一,在大数据这个概念尚未兴起之前,数据已经深入金融行业的多个领域,从最为传统的银行存、贷、汇业务,到保险、信托、证券、基金等领域,以数据为基础的各类金融产品实现了金融资源在不同部门的配置。伴随着数据要素的逐渐投入和信息技术的推广应用,人力、资本等物质要素逐渐被节约,金融运行效率不断提高。尤其是互联网、云计算和人工智能技术上的不断突破,最大程度地释放了数据的流动性。一方面,金融行业在运作中积累的大量数据需要进一步整合、挖掘、统计和分析;另一方面,内外部大数据在金融领域的应用推广,催生了大数据金融的新模式。

1. 大数据的定义

大数据概念兴起于美国。早在 20 世纪 70 年代到 80 年代末,随着计算机技术的发展,数据容量从 Megabyte(MB)达到 Gigabyte(GB)再到 Terabyte(TB)的级别,逐渐超出了单个计算机系统的存储和处理能力,数据并行化技术被提出,主要用于扩展存储能力和提高处理性能。1997 年,美国计算机学会的数字图书馆中出现了第一篇使用“大数据(Big Data)”这一术语的文章——《为外存模型可视化应用控制程序请求页面调度》(迈克尔·考克斯、大卫·埃尔斯沃斯,1997 年)。到了 20 世纪 90 年代末期,Web 1.0 技术的迅猛发展将世界带入了互联网时代,随之带来的是巨量的达到 Petabyte(PB)级别的半结构化和非结构化的网页数据,这需要对迅速增长的网页内容进行索引和查询。尽管并行数据库能够较好地处理结构化数据,但是对于处理非结构化的数据几乎没有提供任何支持。2001 年,美国一家在信息技术研究领域具有权威地位的咨询公司 Gartner 开发了大数据模型。2006 年,由多个软件产品组成的分布式系统基础架构 Hadoop 项目诞生。Hadoop 以其自身在数据提取、变形和加载方面的天然优势得以在大数据处理领域广泛应用。2008 年,美国一些知名计算机科学研究人员组成的计算机社区联盟(Computing Community Consortium)发表了一份有影响力的白皮书——《大数据计算:在商务、科学和社会领域创建的革命性突破》,此组织也是较早提出大数据概念的机构。同年,著名的《自然》杂志出版了一期专刊,专门讨论与未来大数据处理相关的一系列技术问题和挑战。此后,“大数据”逐渐成为互联网信息技术行业的流行词,并引起了各国政府、学术界和产业界的高度关注。但是如何对“大数据”进行界定较难统一,不少文献从不同角度对大数据进行了表述,比较有代表性的有三种:属性定义(Attributive Definition)、比较定义(Comparative Definition)和体系定义(Architectural Definition)。

1) 属性定义

属性定义是从大数据的基本特征出发进行界定,如“3V”“4V”的概括。“3V”是指数量增长的容量(Volume)、多样性(Variety)和速度(Velocity)。“4V”则在“3V”之外增加了价值(Value)特征。

2) 比较定义

比较定义将大数据定义为超过了典型数据库软件工具捕获、存储、管理和分析数据能力的数据集,即大数据是一种规模大到在获取、存储、管理、分析方面大大超出了传统数据库软件工具能力范围的数据集合。这种定义从时间和跨领域比较的角度说明了什么样的数据集才能被认为是大数据,包含了一种演化的观点。

3) 体系定义

美国国家标准和技术研究院(National Institute of Standards and Technology, NIST)认为,“数据的容量、数据的获取速度或者数据的表示限制了使用传统关系方法对数据的分析处理能力,需要使用水平扩展的机制以提高效率”。这种机制就是大数据体系,它可以进一步细分为大数据科学和大数据框架。大数据科学是涵盖大数据获取、调节和评估技术的研究;大数据框架则是在计算单元集群间解决大数据问题的分布式处理和分析的软件库及算法,一个或多个大数据框架的实例化即为大数据基础设施。

归纳以上定义:大数据指无法在一定时间范围内用常规软件工具进行捕捉、管理和处理的数据集合,是需要新处理模式才能具有更强的决策力、洞察发现力和流程优化能力的海量、

高增长率和多样化的信息资产。它包含了以下三层含义。

第一,从资源视角看,大数据是新资源,体现了一种全新的资源观。

随着以 Hadoop 为代表的分布式存储和计算技术迅猛发展,互联网数据管理能力得到了极大的提升,并引发全社会开始重新审视“数据”的价值,开始把数据当作一种独特的战略资源对待,全球数据成指数级增长。

第二,从技术视角看,大数据代表了新一代数据管理与分析技术。

传统的数据管理与分析技术以结构化数据为管理对象,在小数据集上进行分析,以集中式架构为主,成本高昂。与“贵族化”的数据分析技术相比,源于互联网的、面向多元异构数据、在超大规模数据集上进行分析、以分布式架构为主的新一代数据管理技术,与开源软件潮流叠加,在大幅提高处理效率的同时,成百倍地降低了数据应用成本。例如,Hadoop 技术可将数据存储和分析的成本由原来的 3 万美元/TB,压降到 300 至 1000 美元/TB,新一代计算平台 Spark 进一步将 Hadoop 的性能提升了 30 多倍,类似的开源技术,在极大提高了数据分析效能的同时,大大降低了数据分析的技术门槛,为企业提供了低成本的大数据技术方案。

第三,从理念视角看,大数据打开了一种全新的思维角度。

大数据的应用实现了可信、可靠、可验证的境界。首先是“数据驱动”,即经营管理决策可以自下而上地由数据来驱动;其次是“数据闭环”,互联网行业往往能够构建包括数据采集、建模分析、效果评估到反馈修正各个环节在内的完整“数据闭环”,从而能够不断地自我升级、螺旋上升。

当前,国内外缺乏对大数据产业的公认界定。从技术体系的角度来看,市场普遍认同的大数据技术体系包括以 Docker 为代表的容器微服务技术、以 Hadoop 为代表的大规模分布式存储计算技术、以 Spark 为代表的大规模数据分析建模技术、以 Kafka 为代表的消息总线技术、以 HBase 为代表的非结构化查询语言(No Structured Query Language, NoSQL)技术、以 Redis 为代表的内存数据库等。从数据应用的角度来看,大数据产业既包括在大数据采集、存储、管理、挖掘等环节提供数据资源供给、数据分析服务、数据应用产品等“核心大数据企业”,也包括诸多非信息技术领域中,运用大数据理念、技术来提升运作效率,提高决策水平的“大数据生态企业”。

未来,大数据技术将呈现出数据源更丰富、处理技术更强大、分析技术更精准等趋势。数据源方面,经过行业信息化建设,医疗、交通、金融等领域已经积累了大量的数据资源;而随着物联网的应用、移动互联网的普及,来自社交网络、可穿戴设备、车联网、物联网以及政府信息公开平台的数据,将成为大数据增量数据资源的主体。数据处理技术方面,谷歌文件系统(Google File System, GFS)、Hadoop 分布式文件系统(Hadoop Distributed File System, HDFS)技术的出现,奠定了大数据存储技术的基础;而日后出现的 MapReduce、Storm、Dremel、Spark、Pregel 等各类大数据技术,进一步提升了大数据处理能力,在开源社区的不断努力之下,性能更高的新技术将不断涌现,快速更新。数据分析技术方面,大数据为人工智能、深度神经网络的研究突破提供了技术和数据保障。未来,大数据技术不但能够大大降低企业在线分析处理(On Line Analytical Processing, OLAP)、数据挖掘等数据分析工作的成本,更可在大量结构化/半结构化数据以及文字、图片、音频、视频等非结构化数据中获得更多的价值。

2. 大数据特征

大数据特征可用 6V 来描述,如图 3-1 所示。

(1) 大量

大量是指大数据的量非常巨大,具有海量数据规模。

(2) 多样

多样化体现在数据的类型具有多样化方面,除了包括传统的数字、文字外,还有更加复杂的语音、图像、视频等。

(3) 高速

高速是指大数据具有快速的数据流转,必须得到迅速的处理才具有参考价值。

(4) 可变

数据量巨大、种类多等妨碍了处理和有效地管理数据的过程。

(5) 真实

真实是指与传统的抽样调查相比,大数据反映的内容更加全面、真实。

(6) 价值

有价值是指大数据的价值更多地体现在零散数据之间的关联上。

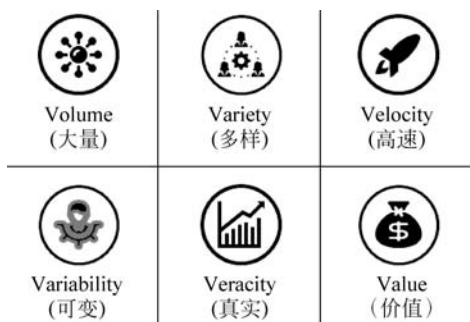


图 3-1 大数据特征

3. 大数据类型

大数据里面的数据分为三种类型。

(1) 结构化数据

即有固定格式和有限长度的数据。例如,填的表格就是结构化的数据。国籍:中华人民共和国;民族:汉;性别:男。这都叫结构化数据。

(2) 非结构化数据

现在非结构化的数据越来越多,就是不定长度、无固定格式的数据。例如网页,有时候非常长,有时候仅有很少的字符;再比如语音、视频也都是非结构化的数据。

(3) 半结构化数据

半结构化数据是一些 XML 或者 HTML 格式的数据。

4. 大数据应用步骤

数据的应用分为四个步骤:数据、信息、知识、智慧,如图 3-2 所示。

5. 大数据分析

若要系统认知大数据,必须要全面而细致地分解它,可着手从三个维度来展开,如图 3-3 所示。

(1) 理论

第一维度是理论,理论是认知的必经途径,也是被广泛认同和传播的基线。在这里从大数据的特征定义理解行业对大数据的整体描绘和定性,从对大数据价值的探讨来深入解析大数据的珍贵所在,洞悉大数据的发展趋势,从大数据隐私这个特别而重要的视角审视人和数据之间的长久博弈。

(2) 技术

第二维度是技术,技术是大数据价值体现的手段和前进的基石。在这里分别从云计算、分

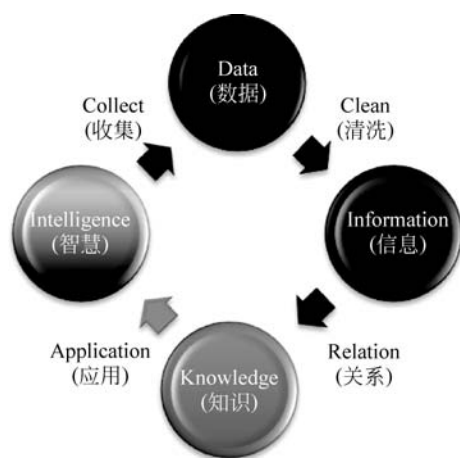


图 3-2 大数据应用步骤

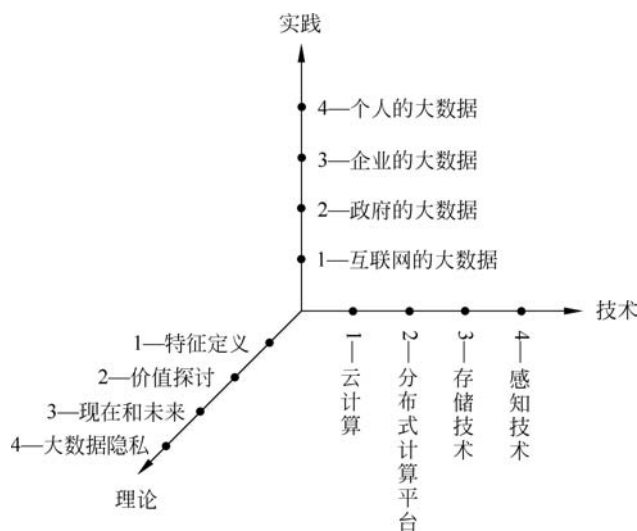


图 3-3 大数据分解

布式处理技术、存储技术和感知技术的发展来说明大数据从采集、处理、存储到形成结果的整个过程。

(3) 实践

第三维度是实践,实践是大数据的最终价值体现。在这里分别从互联网的大数据、政府的大数据、企业的大数据和个人的大数据四个方面来描绘大数据已经展现的美好景象及即将实现的蓝图。

3.1.2 金融行业大数据现状

随着大数据技术的快速发展,大数据在金融行业的应用场景正在逐步拓展,在风险控制、运营管理、销售支持和商业模式创新等细分领域都得到了广泛的应用。

1. 金融行业数据源概览

金融行业内部积累的大数据资源、行业外部获取的大数据资源均可为金融行业所用。按照具体的业务场景,可将金融行业内的的大数据源划分为银行业数据、证券期货业数据、保险业

数据和金融电商平台数据等方面。

(1) 银行业数据

银行业数据主要包括以下五个方面：客户信息数据；由客户交易获取的结构化数据；银行业务处理过程中采集的用于集中作业、集中授权、集中监控的影像、视频等非结构化数据；银行网站访问中隐含的大量客户需求或产品改进信息；各类媒体、社交网络中涉及的银行信息等。

(2) 证券期货业数据

证券期货业的经营对数据的实时性、准确性和安全性的要求较高。证券期货数据包括实时行情、历史金融数据、统计数据、新闻资讯等。数据涵盖股票、期货、基金、债券、股指期货、商品期货等与宏观经济、行业经济息息相关的多个方面。证券期货数据的数据量大、变化快，期货数据每秒更新两次，每日产生上万笔数据。宏观经济数据包括国内宏观经济数据、地区经济数据、行业经济数据、国外宏观经济数据四大类，涉及超过 13 万个经济指标、670 万条经济数据。新闻资讯不仅包括新闻信息和机构研究报告，还包括论坛、微博发布的网络舆情信息，这些数据需要采用网络爬虫、语音分析等非结构化数据处理方法进行数据挖掘。

(3) 保险业数据

保险业数据包括保单、理赔单、电话营销录音、保险业相关行业业务数据、与具体险种相关的行业外数据（气象、经济指标、区域统计指标等）、医疗保险记录和病历、汽车险及投保者的驾驶违章记录数据等。保险业的非结构化数据多为影像数据。这些数据为保险公司的各类决策提供支持，支撑保险营销、定价等业务的开展。

(4) 金融电商平台数据

金融电商平台数据包括支付数据、网络融资服务数据等方面。支付数据即用户的转账汇款、机票订购、火车票代购、保险续费、生活缴费等支付服务数据。网络融资服务数据主要是贷款方的财务报表、运营状况、个人财产等资信相关数据、投资方的个人基本信息和行为信息及偏好信息。从事金融电商业务的公司，除了在自身服务平台上搜集数据外，还可以在互联网上获取如用户的网页浏览数据、其他平台交易数据、网络言论等数据资源，实现对客户的行为进行交叉验证。

2. 国内金融行业大数据应用现状

由于行业的特点，金融行业在“大数据”概念提出之前，就已经是数据治理、数据分析领域的积极实践者，并在数据仓库、数据分析、数据挖掘等领域进行了卓有成效的实践。近年来，金融行业积极吸纳、学习“大数据”理念和相关技术，结合自身业务将已有的数据分析工作推向了新的高度。目前，大数据治理和分析能力已经成为各类金融机构的核心竞争力和发展的主要推动力。

1) 银行业的大数据应用

国内商业银行对数据的集中、规整、分析、挖掘可以追溯到 2000 年前后。近年来，银行 IT 系统建设积极采用大数据所带来的开放、聚合、互联、智能的理念和相关技术体系，取得了一系列应用成果。

(1) 大数据平台建设

实现目标：基于既有的数据仓库或内部数据分析挖掘平台，及时跟进、评估开源社区和大数据行业的技术发展，搭建融合数据仓库和开源技术的大数据处理平台，使得商业银行有能力通过行业内外的数据源开展各类大数据应用。

具体内容：在现有统一的数据库架构下，逐步审慎评估、纳入 Hadoop、YARN、Spark、Tez、HBase、Kafka、OceanBase、NoSQL、内存计算、流计算和图计算等技术，通过使用个人电脑架构服务器，搭建更具经济性的计算集群，以期在数据吞吐量、处理速度、数据源多样性、IT 运维成本等方面获得较高提升，有效支持商业银行在线上、线下各类业务的效率提升和融合。

（2）大数据产品创新

实现目标：基于商业银行多年积累的海量内部数据，纳入合规合法的外部数据，开发出“门槛”更低、更加便捷高效的创新产品，提升产品的竞争力。

具体内容：在多年积累的产品体系基础上，进一步提高内部数据的打通、整合、挖掘水平，纳入覆盖面更广、颗粒度更细的内部数据。借助特征工程、机器学习等大数据分析技术，结合征信、税务、互联网公开数据等外部数据源，在个人、对公信贷、供应链金融等业务场景中进行产品创新尝试，开发出线上申请、快速审批的互联网信贷产品。

（3）大数据风控尝试

实现目标：利用大数据的先进技术，打通内部、外部数据，提升内控合规、反欺诈、信用风险管理等方面的技术水平。

具体内容：采用大数据总线技术，提升数据获取的颗粒度和数据更新速度，借助网络爬虫、图数据库、机器学习等大数据技术，提升数据分析的精度和场景匹配度，全面掌握客户风险情况，提升非现场审计的业务占比。在提高风控质量的同时，有效提升业务效率，减少时间、资金和人力资源的支出。

（4）大数据营销服务探索

实现目标：利用行内积累的客户数据，结合大数据分析技术，准确理解客户需求，发掘潜在客户，提升对客户的感知能力和个性化营销、服务水平。

具体内容：引入非结构化数据处理技术，结合大数据总线技术、机器学习建模、个性化营销技术，利用内部各渠道积累的数据，强化客户行为数据的收集利用，提升数据获取的颗粒度和数据更新速度，通过线上或线下客户经理等通道，准确感知客户的实时需求，并实现全渠道的伴随式服务和营销。

2) 保险业的大数据应用

（1）费率计算模型优化

实现目标：利用过往业务中积累的真实理赔数据，结合内部和外部大数据，通过构建更加精细的模型，实现保费的精准差异化定价，提升盈利能力。

具体内容：利用大数据平台，将内部的客户属性信息、外部获取的客户行为习惯信息与真实的客户理赔数据进行关联，进而使用因子分析、特征工程、逻辑回归、决策树、随机森林等算法，经过多轮数据建模与场景化调优，构建出基于大数据的保费定价模型，对不同理赔概率的客户提供差异化的报价服务。

（2）客户结构优化

实现目标：利用历史积累数据，从既有的客户群中探索出高价值客户群，为进一步优化客户结构提供决策参考。

具体内容：借助关联分析、回归建模、机器学习建模等方法，结合业务规则，对赔付率正常、件均保费高、库存高的客户群体进行精确定位设计专项营销，提升高价值客户群的业务转化率。

（3）好名单优选

实现目标：利用数据挖掘方法进行客户营销转化率分析，区分目标客户的营销转化率，提

升营销成功率。

具体内容：使用回归分析、决策树建模等多变量分析技术，利用既有数据和外部数据资源，对客户进行精准画像，进而以转化率为优化目标，建立营销转化率预估模型，发现转化率高的客户，优先实施精准营销。

（4）基于客户行为的营销资源优化

实现目标：基于历史数据和客户行为数据，实现营销资源的合理配置和有效使用，从而提升营销效果。

具体内容：对营销资源管理系统及历史数据进行分析，结合外部数据，分析客户行为偏好，找出投保最优配置，同时对投保系统进行优化，逐步形成投保全生命周期管理的完整流程。

3）证券业的大数据应用

证券业是典型的数据生产行业和数据驱动型行业，无论是经纪业务中更好地获取客户和为客户提供投资咨询及辅助决策，还是资产管理中的量化投资模型的建立，都已经离不开大数据的有力支撑。

（1）大数据经纪业务

经纪业务作为典型的通道中介，券商服务标准趋同，因此容易陷入价格竞争的红海，而大数据的引入为券商的差异化服务提供支撑，助力券商将经纪业务由通道类业务转变成包含增值服务的金融服务，深刻改变着行业竞争格局。

客户营销：建立潜在客户识别模型和新增客户质量评估模型，制定针对性的营销方案，大大提高拉新效率；对于存量客户，通过建立客户渠道偏好模型、客户购买倾向预测模型、客户投资能力评价模型、产品关联分析模型、客户满意度评价模型和客户忠诚度评价模型等，制定针对性地促进客户活跃度的应对方案，开展相应的营销活动，提高客户活跃度和贡献度。

客户转化率提升：通过对客户交易习惯和行为分析，提升客户交易的频率、客户的资产规模，从而提升业务收益。具体而言，就是根据客户的行为偏好，予以推荐不同的服务。对于交易频率低且年收益率较低的客户，推荐理财产品；对于交易频率高、收益水平高的客户，推送融资服务；对于交易频率低、资金量大的客户，主动提供投资咨询服务。

证券咨询服务：利用数据技术提升投资咨询服务水准，增强客户黏性。例如，基于每日实时抓取的新闻资讯和股票、政经相关数据，通过大数据分析，帮助用户快速获取全网关注的投资热点。

（2）大数据资产管理业务

实现目标：通过构建大数据模型，理顺主力资金与散户资金、主力行为与市场走势、散户情绪与市场走势等的关系，从而增加投资胜率；利用大数据技术，建立针对各个市场、面向不同用户的交易策略，让投资者能够科学稳定地在全球市场投资。

具体内容：利用大数据建立算法交易与量化投资平台，为证券公司资产管理部、证券投资部提供包括高频行情、智能策略交易与交易报盘绿色通道等在内的更加丰富、高效的策略化投资手段；借助大数据技术挖掘历史数据、高频数据和实时分析当前流式数据，通过交易策略的多维运算发现获利机会，根据设定策略全自动委托下单，从而快速完成交易服务，保证执行效率，降低冲击成本。同时实现高端客户的个性化营销，提升客户价值。

4）基金业的大数据应用

大数据的一个重要应用是用来进行辅助投资、制定投资策略。具体来说，大数据可以用来进行选股和准确择时。选股方面，就是利用大数据甄选出基本面向好或投资各关注度较高的

股票并形成投资组合,前者如根据电商网站统计数据购买近期销售向好、价格提升的产品品类的股票,后者如根据财经网站股票板块不同股票浏览数据筛选出近期关注度较高的股票。择时方面,可以利用大数据捕捉投资者的市场情绪,例如根据财经网站股票板块的单击量、关键词如“股票”的搜索量、博客中股票市场文章的发表和单击量等构建情绪指数,在市场情绪上涨时提升组合仓位,在市场情绪回落时降低组合仓位。

5) 互联网金融的大数据应用

互联网金融企业多数为纯线上服务,与客户没有直接接触,它收集客户数据的来源主要分为四类。第一类是自身积累的数据,这主要包括客户在金融服务类网站的行为记录,如电商的交易日志、支付的流水记录,以及一切登录浏览等行为;第二类是通过各类线上、线下的合作伙伴处获取的数据,如行业黑名单、法院审判结果、第三方信用评估等;第三类是通过爬虫从互联网上采集的公开数据,包括新闻、各种空间自媒体、微博;第四类是客户授权从其他系统获得的数据,如客户的信用报告、联系人、工资单、银行流水、电商记录、信用卡流水、通话记录等。这些信息单独存在的价值都不大,但当它们汇聚成海量信息,成为大数据,经过数据采集、清洗、分析,建模、机器学习等一系列步骤后,就可以建立集中式大数据平台,从而提供对应服务。目前大数据在互联网金融行业的应用较为突出的领域有授信、风控反欺诈、营销、动态定价等。

(1) 用户画像

无论是借钱还是投资,企业都需要深入了解客户,包括收入水平、偿还能力、消费偏好、资产配置等,甚至还包括他的心理状况、社会关系、所处行业的趋势等。这些对于客户投资借贷行为的预测都有着至关重要的意义。通过大数据分析,互联网金融企业可以把客户的属性标签从几十个扩展到几百甚至几千个,从而 360 度无死角地描述一个客户。

(2) 快速授信

互联网金融通过大数据等技术手段降低了征信成本和营销成本,使更广泛的人群也拥有了贷款、投资的机会,现在行业小额贷款的审批速度已经普遍达到了十秒甚至秒级。

(3) 风控/反欺诈

互联网在降低金融服务成本的同时,也给金融欺诈打开了方便之门。各种以“钻补贴推广空子”获利的“羊毛党”日益猖獗。身份伪造、恶意逾期等行为,使互联网金融行业损失高达数以十亿元计,每个企业都为如何堵住漏洞、发现欺诈而绞尽脑汁。

小资料 3-1

羊 毛 党

部分群体对搜集各大电子商城、银行、实体店等各渠道的优惠促销活动、免费业务之类的信息产生了浓厚的兴趣。他们有选择地参与活动,从而以相对较低的成本甚至零成本换取物质上的实惠。这一行为被称为“薅羊毛”,而关注与热衷于“薅羊毛”的群体就被称作“羊毛党”。

“薅”意为揪、拔除。“薅羊毛”的典故出自 1999 年央视春晚小品《昨天·今天·明天》上,宋丹丹饰演的白云大妈为了给老伴织一件毛衣,利用给生产队放羊的便利条件,揪羊毛搓毛线,被扣上“薅社会主义羊毛”的罪名。受这一人物的启发,人们便力图把每一分钱都花在刀刃上,享受精打细算乐趣的人群称为“羊毛党”。

开始,“羊毛党”们主要活跃在 O2O 平台或电商平台,随着 2015 年互联网金融的发展,一些网贷平台为吸引投资者常推出一些收益丰厚的活动,如注册认证奖励、充值返现、投标返利等,催生了以此寄生的投资群体,他们也被称为 P2P“羊毛党”。这部分用户与网购“羊毛党”不同,只关注互联网金融产品。

“羊毛党”这个群体在 2017 年频频进入公众视野,泛指针对互联网公司的营销活动,以低成本甚至零成本换取高额奖励的人。由从最初的抢夺免费福利和优惠券,到近年来扎堆 P2P 网贷平台,再到聚集在电商平台上,“羊毛党”也逐渐从分散个体向组团集聚发展,形成了有组织、有规模、有分工的职业“羊毛党”,甚至发展出了完整、成熟的产业利益链。尤其是随着电商之间的竞争越激烈,购物促销活动越来越多,“薅羊毛”的机会也会越来越多。

通过对用户网络行为、设备动态、平台行为、交易行为及整体行为的分析,可以形成一个用户的行为数据图片。例如,通过大数据业务分析和技术分析手段,特别是特征工程能力对这些海量数据进行处理;通过大数据关联叠加后利用特征工程可以找出各种“羊毛党”的行为规则。在识别“羊毛党”后,平台需对“羊毛用户”进一步细化分析,综合评判各细分人群对平台的影响,依照平台的目标制定差异化运营措施,并从技术和业务角度制定相应的运营措施。

欺诈行为包括伪造信息提高授信,利用流程漏洞套利,甚至盗窃、伪造身份骗贷。由于互联网的非接触性和便捷性,使得这种欺诈实施起来更隐蔽,完成起来更迅速。在进行大数据反欺诈时,通常需要多个风控模型协同工作,这里包括基于用户个人申请信息的模型、基于用户社交关系的模型和基于用户历史交易的模型等。同时,还可以使用机器学习模型来自动发掘非线性的特征组合,提高识别的准确率。大数据反欺诈的一个明显优势是,当模型众多、计算量达到一定程度时,结论和数据之间的关系已经无法靠人类经验来解读,这种情况下任何针对单一风控模型的造假就变得极为困难甚至毫无可能。例如,对一些有组织的骗贷行为,使用多个手机号登记、用多个空壳公司为其提供在职证明、填写不同的亲属关系等,利用人工手段进行甄别费时费力,而通过大数据分析就很容易发现这些数据之间的关联,从而进行预警。

(4) 大数据营销

对于金融服务机构来说,它的一个永远的痛点是如何在第一时间洞察客户的金融需求,使用有效手段触达客户,及时推荐最适合的产品,引导客户在本机构完成贷款或投资。

大数据在营销方面的一个解决方案包括分析信贷产品、洞察目标客群、做客群画像;通过意愿预测模型,预测客户意愿;对客户进行分层,不同价值等级采取不同的营销手段;结合客群共同特征进行营销模板的设计;实时性的数据反馈,进行模型的优化迭代;对客户动态分析,帮助风控建模及交叉营销。由于结合了大数据的精准营销模式,整体响应率、符合率都比传统模式有较明显的提升,模型逐步地优化迭代,各环节营销效果也是呈上升趋势。

(5) 动态定价

动态定价是指抛开传统的围绕产品的固定定价模式,将价格与服务的场景、对象绑定在一起,更精准地用价格杠杆应对风险,达到提高收益的目的。这个应用的典型例子是保险产品运费险。通过大数据分析,让保险公司能够针对具体的人和商品来进行定价。具体来说,就是通过对退货风险的大数据分析,发现退货概率和消费者属性及消费场景的内在关联关系,例如,女性更容易退货,鞋类退货率高。再通过数据建模和深度学习,制定出总收益最高的保险费策略。于是,对低退货风险的人和商品,运费险只要几角钱,而在高退货风险的情况下,运费险甚

至可能比商品价格还贵,最终保险公司提高了收益。另一个目前开始流行的动态定价应用是动态利率。对于同一类信贷产品,针对不同用户,甚至针对不同场景下的同一个用户,都可以实现利率实时计算,而不是基于某种预先设置的静态策略。

6) 大数据的流通

国外大数据流通市场始于2008年前后,得益于较为完善的法律制度、信用体系和数据开放环境,企业间数据交易较为活跃。根据《2016 大数据全景图》(马特·图尔克,美国第一标记(First Mark)风险投资公司),国外规模以上数据经纪服务企业有70多家,包括推特(Twitter)、领英(LinkedIn)、甲骨文(Oracle)、微软(Microsoft)、富士通(Fujitsu)等企业都已有涉足。

国内大数据流通市场起步于2010年,尚处于初始阶段。在交易所建设方面,2015年4月14日,全国首个大数据交易所——贵阳大数据交易所正式挂牌运营并完成首批大数据交易。由上海经济和信息化委员会指导的上海大数据交易中心也于2016年4月1日挂牌成立。此外,诸如北京数海科技、数据堂、北京腾云天下科技有限公司、中关村大数据产业联盟等企业和产业联盟在数据交易流通领域也开始布局。

对于敏感度较高的金融行业大数据,其流通价值是可以预见的。业界普遍认为,必须要依托政府和市场的双重力量,由数据供方、数据平台、数据需方和监管机构四方参与的数据交易机构作为兼具“技术、信息安全和法律保障”的数据价值转化渠道,才可以有效规范数据交易行为,实现商业价值、个人隐私和公共利益的平衡。

3.1.3 金融大数据发展展望

1. 金融行业内部、外部数据的融合力度进一步加强

金融行业的信息化程度较高,并已在多年的数据治理过程中积累了丰富的数据资产。近年来,一些金融机构已经尝试多种跨界合作的场景,并在其中尝试接入税务、工商和运营商等外部数据,实现内部金融数据与外部行业数据的融合,已经初步发掘了大数据融合的协同价值。

与此间时,一批非金融企业进入金融服务领域,这些“外来者”过去往往在行业中已经有很深的沉淀,或多或少也积累了一定量的数据。进入金融领域后,原有数据被重新梳理,从另一个角度审视其数据价值。原有行业数据的金融短板也要求企业引入更多的数据,通过跨界融合产生新的数据应用场景。

未来,金融行业内部、外部数据将进一步融合,大数据应用将获得更全面、细致的数据基础,从而推动更多基于大数据的金融业务创新。

2. 大数据对金融业务的驱动作用进一步显现

近两年,金融机构在充分消化、吸收大数据技术的基础之上,利用大数据的理念与技术,开展了一系列的大数据应用。从用户画像深入到用户特征分析,并通过不同角度的业务特征分析。把数据应用扩展到日常运营、产品创新、风险控制、个性化客户服务等主要的业务领域。在一些业务领域中,大数据已经深度融入业务流程的计划、执行、监控、评估等环节,形成了业务大数据的完整闭环。通过大数据闭环,甚至可以快速验证数据应用的效果和价值。

大数据与人工智能将推动新一波金融创新。诸如深度学习、图分析、自然语言处理、语音识别、图像内容理解等技术也在快速演进,将会逐渐发展成为金融细分业务的数据驱动引擎。智能投资、精准营销、反欺诈、反黑产等数据引擎也已经进入实战阶段,显现出很高的业务价

值。未来,越来越多的精细化、全流程的闭环业务驱动引擎将会出现,在金融经营活动的各个领域发挥价值,提升金融机构的经营效能。

3. 金融机构与大数据服务机构的合作进一步深化

近年来,一些金融机构与专业的大数据服务机构合作,将自身对金融业务、客户市场的深度理解与大数据服务机构的数据资源整合能力、大数据技术实践能力结合起来,共同研发出了新颖、实用、高效的大数据金融应用,获得了市场与客户的共同认可。在这一过程当中,一批技术过硬、依法合规开展大数据服务的新型专业机构不断涌现。这类以大数据服务作为主营业务的新兴机构,往往能够在金融机构的细分业务领域提供数据技术层面的各种技术工具和技术服务,从而实现价值。

金融大数据的应用开发唯快不破,面对激烈的市场竞争,越来越多的金融机构将与数据交易市场、数据应用提供商、数据驱动引擎开发商等专业大数据服务机构进行合作,从数据获取、存储、分析、呈现等各个层面上开展协同创新,共同发掘金融服务的新价值。新兴大数据服务机构将由此成为金融大数据生态的重要组成部分荣登大雅之堂。

3.2 云计算技术

3.2.1 云计算概述

1. 云计算的概念

云计算(Cloud Computing)是由分布式计算(Distributed Computing)、并行处理(Parallel Computing)、网格计算(Grid Computing)发展而来的,是一种新兴的商业计算模式。目前,人们对云计算的认识在不断的发展变化之中,因此尚未形成对云计算普遍一致的定义。

我国有学者对于云计算给出如下定义:云计算将计算任务分布在由大量计算机构成的资源池中,使各种应用系统能够根据需要获取计算力、存储空间和各种软件服务。

通俗的理解是,云计算中的“云”就是存储于互联网服务器集群中的资源,它包括硬件资源(如服务器、存储器、中央处理器等)和软件资源(如应用软件、集成开发环境等),本地计算机只需要向互联网发送一个需求信息,远端就会有成千上万台计算机为其提供所需的资源并将结果返回到本地计算机,这样本地计算机几乎不需要做什么,所有的处理都由云服务提供商所提供的服务器集群来完成。

狭义的云计算是指基础设施的交付和使用模式,即通过网络按照需求、易扩展的方式获得所需的资源(包括硬件、平台、软件)。提供资源的网络被称为“云”。“云”中的资源在使用者看来是可以无限扩展的,并且可以随时获取,按需使用并付费。通常将这种特性称为像使用水、电一样使用 IT 基础设施。

这个 IT 基础设施包括计算资源(云计算)、网络资源(虚拟网络)、存储资源(云储存)三个方面,如图 3-4 所示。

(1) 计算资源

假如你要买一台电脑(台式计算机或笔记本电脑),这台电脑是什么样的 CPU? 多大的内存? 这两个就被称为计算资源。

(2) 网络资源

你买的电脑要上网,就需要有一个可以插网线的网口,或者有可以连接路由器的无线网卡。你需要到运营商去开通一个宽带网络,比如中国联通、中国移动或者中国电信等。然后会

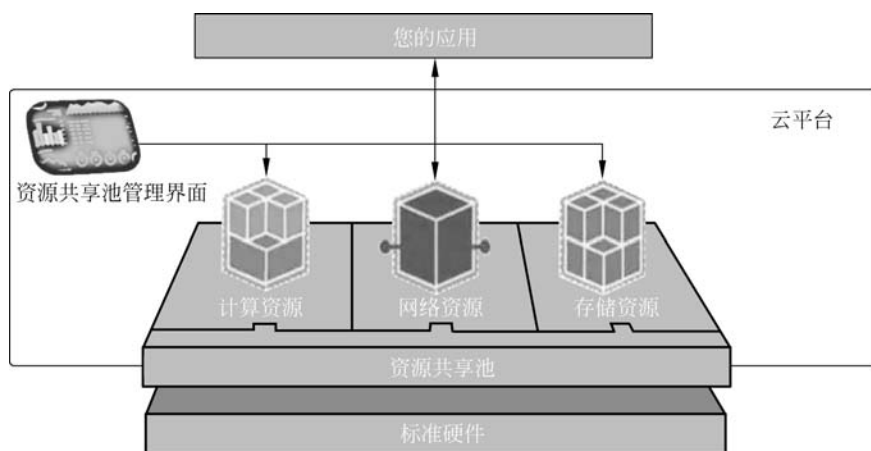


图 3-4 云计算的 IT 基础设施

有工作人员到你家来安装一条网线,并将你的路由器和该运营商的网络连接配置好。这样你家中的所有的电脑、手机、平板电脑就都可以通过路由器上网了,这就是网络资源。通过云平台可以在灵活的时间(随时)内提供灵活的空间(任意大小)的网络资源,即建立虚拟网络。

(3) 存储资源

你买的电脑硬盘内存多大? 过去的硬盘内存都很小,如 10GB; 后来即使 500GB、1TB、2TB 的硬盘也很普通。这就是存储资源。云平台可以根据用户的需求,随时(时间灵活性)提供任意大小(空间灵活性)的存储资源,即云存储。

广义的云计算是指服务的交付和使用模式,即通过网络按需且易扩展的方式获得所需的服务。这种服务可以是 IT 基础设施,也可以是其他服务。云计算技术在网络服务中随处可见,如搜索引擎,用户只要输入简单的指令即可得到大量的信息。

2. 云计算的特点

云计算具有大规模、分布式、虚拟性、可用性、扩展性、个性化、低成本、安全性等特点,如图 3-5 所示。

(1) 大规模

“云”一般具有相当的规模,一些著名的云服务提供商,如谷歌、亚马逊、IBM、微软等都拥有百万数量级的服务器规模。而依靠这些服务器构建起来的“云”能够为用户提供强大的计算能力。

(2) 分布式

云计算是透过网络将庞大的计算处理程序

自动分拆成无数个较小的子程序,再交由多台服务器(被分布在众多的服务器主机上)所组成的庞大系统,通过分布式计算分析之后,再将处理结果回传给用户。

(3) 虚拟化

云计算采用虚拟化技术,用户并不需要关注具体的硬件实体,只需要选择一个云服务提供商,注册并登录到它的云控制台上,去购买所需要的服务(如云服务器、云存储、内容分发网络等),再为所购买的服务做相应的配置,然后就可以使用自己的操作和应用了。这不仅比到企



图 3-5 云计算特点

业的数据中心去部署一套应用系统要简单和方便得多,而且用户还可以随时随地通过个人计算机或移动设备来控制资源,这就好像是云服务提供商为每个用户都提供了一个互联网数据中心(Internet Data Center, IDC)一样。

(4) 可用性

大的云服务提供商一般都会采用数据多副本容错、计算节点同构可互换等措施来保障服务的高可靠性。基于云计算的应用甚至可以持续(7×24 小时)不间断地对外提供服务。

(5) 扩展性

“云”的规模可以动态伸缩,以满足应用和用户规模增长的需要。

(6) 个性化

用户可以根据自己的需要来购买服务。

(7) 低成本

用户可以按使用量来精确付费。这可以大大降低用户的使用成本,而资源的整体利用率也将得到明显的改善。

(8) 安全性

网络安全已经成为所有企业或个人创业者都必须面对的问题,企业或个人很难应对那些来自网络的恶意攻击,而使用云服务则可以借助更专业的安全团队来有效降低安全风险。

3. 云计算的分类

对于云计算而言,不同的视角有不同的分类方式,分类结果也不同。按照服务类型分类,可以将云计算分为软件即服务、平台即服务和基础设施即服务三种类型;按照部署类型分类可分为公共云、私有云和混合云三种,如图 3-6 所示。



图 3-6 云计算的分类

1) 按照服务类型分类

按照服务类型可以将云计算分为软件即服务(Software as a Service, SaaS)、平台即服务(Platform as a Service, PaaS)和基础设施即服务(Infrastructure as a Service, IaaS)等三种。

(1) 软件即服务

这种类型的云计算是指 SaaS 提供商将应用软件统一部署在自己的服务器上,用户根据需求通过互联网向其订购应用服务;SaaS 提供商根据用户所订购的软件的数量、时间的长短等因素收费,并且通过浏览器向用户提供应用软件。它的优势是,由服务提供商维护和管理应用软件,提供应用软件运行的硬件设施,用户只要拥有能够接入互联网的终端,即可随时随地使用应用软件。在这种模式下,用户不再像传统模式那样在硬件、软件、维护人员等方面花费大量的资金,而只要支出一定的费用,通过互联网就可以享受到相应的硬件、软件和维护服

务,这是效益最高的网络应用运营模式。

对于小型企业来说,软件即服务模式是使用先进技术的最好途径。以企业管理软件为例,基于软件即服务模式的 ERP 系统可以根据并发用户数量、所用功能种类、数据存储容量、使用时间长短等因素来计算用户需要支付的服务费用。用户既不需要支付软件许可费用,承担软件开发、实施费用以及系统维护费用,也不需要购买服务器等硬件设备以及操作系统、数据库等系统软件。实际上,基于软件即服务模式的 ERP 系统正是继承了开源 ERP 系统免许可费用,而只收服务费用的重要特征,是突出服务的 ERP 系统。

Salesforce 是典型的软件即服务产品,Google Docs、Google Apps 和 Zoho Office 也属于这类服务。

(2) 平台即服务

这种类型的云计算把开发环境作为一种服务来提供。这是一种分布式平台服务,PaaS 服务提供商向用户提供开发环境、服务器平台、硬件资源等服务,用户基于其平台定制开发自己的应用软件并通过其服务器和互联网传递给其他用户。这种模式能够向企业或个人提供中间件平台、应用软件开发数据库、服务器、托管等服务。

Google App Engine、八百客的 800App 都是典型的平台即服务产品。以 Google App Engine 为例,它是一个由 Python 应用服务器群、BigTable 数据库及 GFS(Google File System,谷歌文件系统)组成的平台,为用户提供了一体化主机服务器及可自动升级的在线应用服务。用户编写应用程序并将其运行于 Google 的基础架构之上就可以为其他互联网用户提供服务,在此过程中 Google 提供应用程序运行和维护所需要的平台资源。

(3) 基础设施即服务

这种类型的云计算把 IaaS 提供商的由多台服务器组成的“云”基础设施,作为计算服务提供给用户。它将内存、输入/输出设备、存储和计算能力整合成一个虚拟的资源池,为整个业界提供所需要的存储资源和虚拟化服务器等服务。这是一种硬件托管型的服务方式,用户付费使用服务提供商的硬件设施。例如,Amazon 的 Amazon Web 服务(AWS)、IBM 的 Blue Cloud 等均是基础设施作为服务出租。

基础设施即服务模式的优点是用户只需要购买低成本的硬件,按需租用 IaaS 提供商提供的计算和存储服务,因而大大降低了在硬件上的开销。Google Cloud 是典型的基础设施即服务。

一个典型的云计算系统架构如图 3-7 所示。

2) 按照部署类型分类

按照部署类型可将云计算分为公共云、私有云和混合云三种。

(1) 公共云

人们所说的“云”一般都是指公共云。公共云使用虚拟化和网络技术来提供按需扩展的计算和存储服务。世界上许多基础设施都依赖公共云基础架构。

(2) 私有云

为了应对用户单独使用企业基础设施的需求,云服务提供商开始提供私有云,这些私有云具有许多与公共云相同的特点。两者的主要区别在于私有云是一个组织拥有并控制所有云服务器。自定义私有云使组织能够在安全和私密的环境中充分利用虚拟化的优势,集中管理和弹性调度资源。

(3) 混合云

公共云和私有云是互补的技术,许多企业基础设施用户都需要使用这两种技术,因此产生

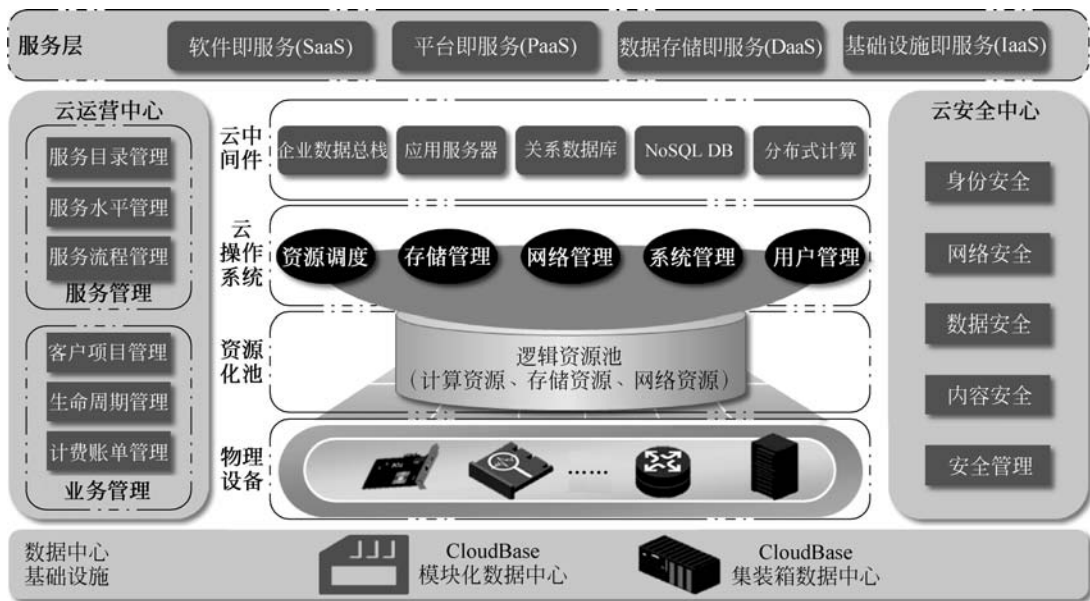


图 3-7 云计算系统架构

了混合云。混合云集成了公共云和私有云平台,既可以提供私有云的安全性,又可以提供公有云的计算资源,从而有效地降低了成本。

4. 云计算平台与传统 IDC 服务平台的区别

与传统 IDC 服务平台相比,新兴的云计算平台具有运行成本低、开放度高以及无限扩容等优点。不仅如此,由于云计算平台是基于互联网的虚拟化计算平台,因此用户可以随时随地享受云计算带来的便利。云计算平台与传统 IDC 服务平台的区别主要体现在以下几个方面。

(1) 服务类型方面

传统 IDC 服务平台可以分为实体服务器托管和租用两种类型。实体服务器托管是指由用户自行购买硬件设备,并将其放到 IDC 服务平台的机房中进行托管,而且在托管期间硬件设备的管理和运行都由用户自己完成,IDC 服务平台主要提供 IP 接入、带宽接入和电力供应等服务。租用是指 IDC 服务平台不仅提供管理服务,也向用户提供服务器,用户无须自行购买硬件设备就可以使用 IDC 服务平台所提供的计算和存储服务。但是,云计算平台提供的是从 IT 基础设施到业务基础平台再到应用层面的连续一体化的全套服务。所以与传统服务平台相比,云计算的效率更高,用户更省心。

(2) 开放性方面

与互相孤立、无法共享的传统 IDC 服务平台相比,云计算平台在资源共享、信息互通等方面做得比较好,而且极具开放性。

(3) 扩展性方面

传统 IDC 服务平台的扩展需要占用大量的机房和场地,而且其处理能力有一个临界值,在达到这个临界值后再增加服务器的数量,处理能力也不会有很大提升。云计算平台则与之不同,云计算平台的资源是动态扩展的且是虚拟化的形式,所以从理论上说云计算平台具有无限扩展性。

(4) 运行成本方面

基于开源软件构建云计算平台可以大幅降低购买硬件设备,以及运行和维护系统的成本。另外,“云”是一个庞大的资源池,用户可以按需购买。也就是说,云计算平台可以像水、电、煤气等资源那样,根据用户的实际使用情况来计费。

5. 云计算的核心技术

云计算平台使用了许多技术,其核心技术有编程模型、海量数据分布存储技术、海量数据管理技术、虚拟化技术和云计算平台管理技术,如图 3-8 所示。



图 3-8 云计算的核心技术

(1) 编程模型

MapReduce 是谷歌开发的 Java、Python、C++ 编程模型,它是一种简化的分布式编程模型和高效的任务调度模型,用于大规模数据集(大于 1TB)的并行运算。严格的编程模型使得在云计算环境下进行编程十分简单。MapReduce 的指导思想是将要执行的问题分解成 Map(映射)和 Reduce(化简),先通过 Map 程序将数据切分为不相关的区块,并将这些区块分配(调度)给大量计算机去处理,达到分布式运算的效果,再通过 Reduce 程序将结果汇总输出。

(2) 海量数据分布存储技术

云计算平台由大量的服务器组成,同时为大量用户服务,因此云计算平台用分布式存储的方式存储数据,用冗余存储的方式保证数据的可靠性。云计算平台中广泛使用的数据存储系统是 Google 文件系统 GFS 和 Hadoop 分布式文件系统 HDFS。

GFS(Google File System)是一个可扩展的分布式文件系统,用于大型的、分布式的、对大量数据进行访问的应用。GFS 的设计思想不同于传统的文件系统,它是针对大规模数据处理和 Google 应用特性而设计的。GFS 虽然运行于普通的硬件设备上,但可以为大量用户提供总体性能较高的服务。

一个 GFS 集群由一台主服务器(Master)和大量的块服务器(Chunk Server)构成,并被许多客户(Client)访问。主服务器存储有整个文件系统的元数据,包括名字空间、访问控制信息、从文件到块的映射,以及块的当前位置。它还控制了一些系统层面的活动,如块租约(Lease)管理、孤儿块的垃圾收集,以及块服务器间的块迁移。主服务器定期通过心跳(Heart Beat)消息与每一台块服务器通信,向块服务器传递指令并收集它们的状态。CFS 中的文件被切分为 64MB 的块并以冗余存储的方式存储,每块数据在系统中保存 3 个以上的副本。

客户与主服务器的交换只限于对元数据的操作,所有数据方面的通信都直接和块服务器联系,这就大大提高了系统的效率,同时防止主服务器负载过重。

(3) 海量数据管理技术

云计算需要对分布的、海量的数据进行处理、分析,因此数据管理技术必须能够高效地管

理大量的数据。

云计算平台中的数据管理技术主要是 Google 的 BT(BigTable)数据管理技术和 Hadoop 的开源数据管理模块 HBase。BigTable 是建立在 GFS、Scheduler、Lock Service 和 MapReduce 之上的一个大型分布式数据库,与传统的关系数据库不同,它将所有数据都作为对象来处理,从而形成一个巨大的表格,用于存储大规模结构化数据。谷歌的很多项目都使用 BigTable 来存储数据,包括 Google 搜索、Google 地球和 Google 金融。这些应用程序对 BigTable 的要求各不相同:数据大小(从 URL、网页到卫星图像)不同,反应速度不同(从后端的批处理到实时数据服务)。对于不同的要求,BigTable 都可以提供灵活、高效的服务。

(4) 虚拟化技术

通过虚拟化技术可以将软件应用与底层硬件相隔离,它既包括将单个资源划分成多个虚拟资源的裂分模式,也包括将多个资源整合为一个虚拟资源的聚合模式。按照虚拟的对象可以将虚拟化技术分成存储虚拟化、计算虚拟化、网络虚拟化等,其中计算虚拟化又分为系统级虚拟化、应用级虚拟化和桌面虚拟化。

(5) 云计算平台管理技术

云计算平台的资源规模庞大、服务器数量众多且分布在不同的地点,同时运行着诸多的应用程序。如何有效地管理这些服务器,保证整个系统能够提供不间断的服务,是一个巨大的挑战。

云计算平台管理技术能够使大量的服务器协同工作,快速发现和恢复系统故障,通过自动化、智能化的手段实现大规模系统的可靠运营,同时也方便用户部署和开通应用。

3.2.2 云计算应用与发展

1. 云计算的发展

任何一次技术创新的规模化过程都是漫长的,事实上在 20 世纪 70 年代就有了云计算的雏形,但直到 2007 年以后云计算才开始迅速发展。

1963 年,美国国防部高级研究计划署向麻省理工学院提供了约 200 万美元的津贴启动了著名的 MAC(Multiple Access Computer)项目,要求其开发“可多人同时使用的计算机系统”技术。当时,麻省理工学院就构想了“计算机公共事业”,即让计算资源能够像电力一样供应,由此产生了“云”和“虚拟化”技术的雏形。

在“云”和“虚拟化”技术雏形已经具备的前提下,还需要用网络来作为媒介,如果没有网络,这些构想就都只是空中楼阁。1969 年,ARPANET 诞生了,并成功完成了两台计算机之间的数据传输试验,这就是今天互联网的雏形。互联网的诞生也使得云计算从理论走向现实。

随后,随着互联网的发展,以及从 20 世纪 90 年代开始虚拟计算机的逐渐流行,云计算基础设施得到迅猛发展。

总的来说,云计算的发展主要经历了 4 个阶段,这 4 个阶段依次是电厂模式、效用计算、网格计算和云计算,如图 3-9 所示。

(1) 电厂模式阶段

电厂模式类似于利用电厂的规模效应来降低电力的价格,使用户无须维护和购买任何发电设备,而且使用起来更加方便。处于电厂模式阶段的云计算,将大量分散的资源集中在一起,并对它们进行规模化管理,从而降低了用户的使用成本,也让用户使用起来更加方便。

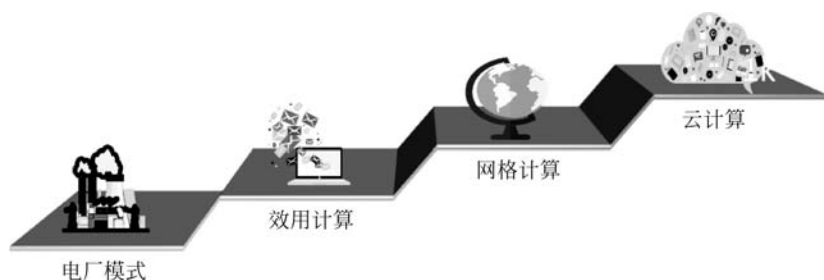


图 3-9 云计算的发展阶段

（2）效用计算阶段

20 世纪 60 年代初,计算设备的价格非常高昂,一般的企业、学校和机构难以承受,所以人们产生了共享计算资源的想法。1961 年,人工智能之父麦肯锡在一次会议上提出了“效用计算”的概念,其核心思想借鉴了电厂模式,目标是整合分散在各地的服务器、存储系统以及应用程序供多个用户共享,让用户能够像把灯泡插入灯座那样方便地使用计算资源,并且根据用户的使用量来计费。

（3）网格计算阶段

网格计算是研究如何把一个需要巨大计算能力才能解决的问题分成许多小的部分,然后将这些小的部分分配给许多性能较低的计算机来处理,最后将计算结果汇集起来去解决大问题。但是,由于网格计算在商业模式、技术和安全性方面存在不足,使得其并没有在工业界和商业界取得预期的成功。

（4）云计算阶段

云计算与效用计算和网格计算类似,也是希望使用计算资源能够像使用电那样方便,而且成本低廉,但是与效用计算和网格计算不同的是,目前云计算在技术方面也已经基本成熟,而且应用也有了一定的规模。

2. 云计算应用领域

云计算的应用主要在物联云、安全云、存储云、游戏云、计算云、金融云、医疗云、教育云 8 个领域,如图 3-10 所示。

（1）物联云

物联网是互联网的发展和延伸,使原来的人与人、人与物的互联发展到物与物的互联。物联网的运用和发展是科技进步、社会不断发展的产物,云计算在其中的信息处理和运用方面发挥着十分重要的作用。

（2）安全云

安全云(Security Cloud)是一个由“云计算”演变而来的词汇。安全云的策略是使用者越多,每个使用者就越安全,庞大的用户群犹如一个恢恢天网覆盖互联网的每一个角落,只要新病毒一出现,立刻就会被发现和截获。

（3）存储云

存储云是通过虚拟化、网格计算或分布式文件系统等技术,将网络中各种类型的硬件存储设备通过特定的软件集合起来协同工作,共同对外提供数据存储和业务访问功能的系统。如



图 3-10 云计算主要应用领域

果云计算平台的主要任务是对大批量数据进行存储和管理,就需要在云计算平台中配置大量的硬件存储设备,那么云计算平台就成为云存储平台。所以,云存储是一个以数据存储和管理为核心的云计算平台。

(4) 游戏云

游戏云是以云计算技术为支撑的一种游戏方式。在游戏云的运行模式下,所有游戏都在服务器端运行,经过渲染处理的游戏画面被压缩后通过网络传送给游戏用户。在客户端,用户的游戏设备不需要一定是高端处理设备,只要具备基本的视频解压缩功能就可以得到具有很好视觉效果的游戏画面。

(5) 计算云

从技术上看,云计算与大数据的关系就像一枚硬币的正反面一样密不可分。大数据无法用单一的计算机进行处理,而必须采用分布式计算体系。大数据的特色在于对海量数据的深度挖掘,但它必须依托云计算的分布式处理技术、分布式数据库管理技术、云存储技术和虚拟化技术。

(6) 金融云

金融云是指利用云计算的模型,将信息、金融和服务等功能分散到庞大分支机构构成的互联网“云”中,旨在为银行、保险和基金等金融机构提供互联网处理和运行服务,同时共享互联网资源,从而解决现有的各种问题并且达到高效、低成本的目标。现在已基本普及了的快捷支付,因为有了金融与云计算的结合,只需要在手机上进行简单操作,就可以完成银行存款、购买保险和基金买卖。现在,像苏宁金融、腾讯等企业均推出了自己的金融云服务。

(7) 医疗云

医疗云是指在云计算、移动技术、多媒体、通信、大数据以及物联网等新技术基础上,结合医疗技术,使用“云计算”来创建医疗健康服务云平台,实现医疗资源的共享和医疗范围的扩大。因为云计算技术的运用与结合,医疗云提高了医疗机构的效率,方便居民就医。像现在医院的预约挂号、电子病历、医保等都是云计算与医疗领域结合的产物,医疗云还具有数据安全、信息共享、动态扩展、布局全国的优势。

(8) 教育云

教育云可以将所需要的任何教育硬件资源虚拟化,然后将其输入互联网中,即可向教育机构和学生老师提供一个方便快捷的平台。现在流行的慕课就是教育云的一种应用。慕课(MOOC)指的是大规模开放的在线课程。在国内,中国大学 MOOC 就是非常好的教育云平台。在 2013 年 10 月 10 日,清华大学推出了 MOOC 平台——学堂在线,许多大学现已使用学堂在线开设了部分课程的 MOOC。

3. 云计算发展中存在的问题

云计算尽管具有许多优点,但是也存在一些问题,如访问权限问题、信息保密问题、用户使用习惯问题、网络传输问题等。

(1) 访问权限问题

用户可以在云计算服务提供商处上传自己的数据资料,相比于传统的利用个人计算机或硬盘的存储方式,此时需要建立账号和密码完成虚拟信息的存储和获取。这种方式虽然为用户的信息资源获取和存储提供了方便,但用户失去了对数据资源的控制,而服务商则可能存在对资源的越权访问状况,从而造成信息资料的安全难以保障。如何保证存放在云计算平台上的数据不被非法利用,这不仅需要技术方面的改进,也需要法律法规的进一步完善。

(2) 信息保密问题

信息保密性是云计算技术的首要问题,也是当前云计算技术的主要问题。比如,用户的资源被一些企业进行资源共享。网络环境的特殊性使得人们可以自由地浏览相关信息资源,信息资源泄漏是难以避免的,如果信息保密性不足就可能严重影响到信息资源的所有者。

(3) 用户使用习惯问题

改变用户的使用习惯,使用户适应网络化的应用环境是长期而艰巨的任务。

(4) 网络传输问题

云计算服务依赖于网络,如果网速低且不稳定,云计算的性能就很难提高。可见,云计算服务的普及依赖于网络技术的发展。

(5) 数据完整性问题

在云计算技术的使用中,用户的数据被分散存储于云计算数据中心的不同位置,而不是某个单一的系统中,数据资源的整体性受到影响,使其作用难以有效发挥。另一种情况就是,服务商没有妥善、有效地管理用户的数据信息,从而造成数据存储的完整性受到影响,信息的应用作用难以被发挥。

(6) 法律法规不完善

云计算技术相关的法律法规不完善也是存在的主要问题之一,要实现云计算技术作用的有效发挥,就必须对其相关的法律法规进行必要的修订。目前来看,法律法规尚不完善,云计算技术发挥作用仍然受到制约。就当前云计算技术在计算机网络中的应用来看,其缺乏完善的安全性标准,缺乏完善的服务等级协议管理标准,没有明确的责任人承担安全问题的法律责任。另外,缺乏完善的云计算安全管理的损失计算机制和责任评估机制。法律规范的不足和缺失也制约了各种相关活动的开展,导致计算机网络的云计算安全性难以得到保障。

3.2.3 金融行业云计算应用现状

当前,云计算已引发金融领域重大变革,是金融科技的重要组成部分。

1. 云计算加速金融行业 IT 架构转型

受多种因素的影响,长期以来我国金融业的关键核心业务信息系统、灾备系统等主要基于国外高端软硬件。这些高端软硬件有力地推动了我国金融业的发展。然而,在“互联网+”时代,业务的转型发展对 IT 系统的安全性、可用性与业务持续性提出了更高的要求,基于上述因素,国外高端软硬件技术架构的弊端逐渐显现,主要表现在以下 4 个方面。

(1) 建设和运维成本偏高

多数金融机构一直以来采用最成熟、可靠的 IT 技术路线,通常使用国外主流厂商提供的信息技术和商业产品来进行集中式部署。由于在信息技术实施、支持和保障上很大程度依赖于信息技术供应商,从而存在着技术标准不统一、新技术应用和技术创新缓慢、投入产出比低下等问题,同时也使得金融机构自身缺乏核心技术积累,在技术路线选择上受制于国外厂商,并被某几大国外公司垄断。随着国内基础设施规模的扩大,导致数据中心建设成本不断攀升。

(2) 资源交付效率低

随着金融服务互联网化、移动化的发展趋势,以及互联网金融公司竞争、利率市场化等的挑战,金融机构从战略和战术上积极应对,提出了互联网金融、大数据、电子商务等新的战略目标,并以此加速业务模式创新。但这些目标所需要的海量信息技术处理能力往往无法通过传

统 IT 基础设施解决方案有效满足,即使传统方案能够实现,企业也难以承受漫长的建设周期。因此,要满足新业务发展的响应速度,必须加快采用新技术。

(3) 资源调整不灵活

金融机构在传统系统架构下资源分配往往是固定的,是按照单个应用系统资源需求进行建设和部署,资源之间形成孤岛,不能灵活调整。例如,在淘宝“双 11”促销和电商秒杀等业务需求中,传统技术架构只能按照业务峰值配置基础设施资源,造成巨大的资源浪费。随着互联网金融、电子商务等业务快速发展,对基础设施资源的灵活调整、弹性伸缩提出了更高的要求。

(4) 运行风险日益突出

金融机构数据中心作为“金融业跳动的的心脏”,稳定运行和控制风险是第一要务。一方面,基础设施故障、突发业务压力、频繁变更上线等均可能影响系统的稳定和服务质量,而随着业务部门和金融监管机构要求的不断提高,对数据中心高可用性的要求日益严格;另一方面,数据中心对外部基础设施、外部技术和服务的依赖性不断增强,网络入侵、信息泄露等安全风险日益突出。

相反地,近几年来国内外云计算发展十分迅猛,除了新兴的云计算厂商在大力推动云计算发展之外,一些传统 IT 厂商也纷纷向云计算转型,云计算技术和服务越来越成熟、越来越开放和标准化,逐渐在多个领域广泛应用。

正是在这种新旧技术交替发展的过程中,我国金融业也在悄然发生改变,一些新兴金融机构迫于成本、人力的压力,直接使用云计算服务,有力支撑了业务快速增长;与此同时,一些传统金融机构为应对移动互联网时代下的金融业务发展需求,也在探索向云计算、分布式架构转型。

2. 金融行业云架构

根据使用云计算平台的客户范围不同,金融行业的云架构模式可以分为公共云、专有云、混合云和行业云(如金融云),如图 3-11 所示。

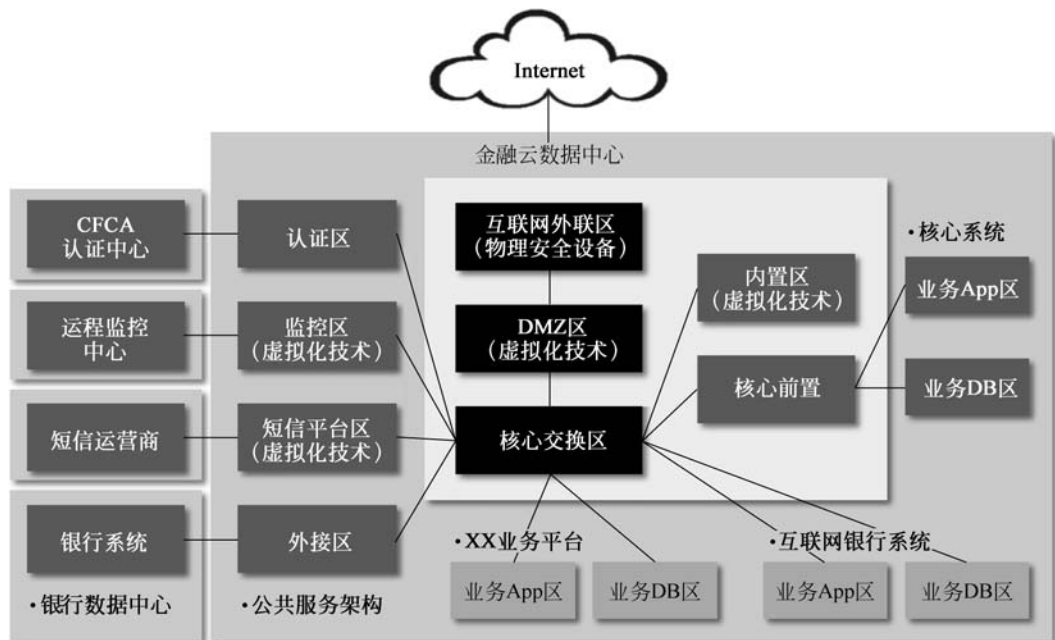


图 3-11 金融行业云架构

(1) 公共云

公共云指不限制客户范围的云计算平台。

(2) 专有云

专有云指专为某个机构服务的云计算平台。

(3) 混合云

混合云指前述几种部署模式的组合。

(4) 行业云

行业云(即金融云)主要指仅限于为金融行业服务的云计算平台,包括金融机构自建的专有金融云、云服务商为金融业提供的公共金融云,以及上述两种模式组合的混合金融云。

3. 金融业云计算应用特点

金融机构应用云计算服务有如下特点。

(1) 减少开销和能耗

采用云计算服务可以将硬件和基础设施建设资金投入转变为按需支付服务费用,客户只对使用的资源付费,无须承担建设和维护基础设施的费用,避免了自建数据中心的资金投入。云平台使用虚拟化、动态迁移和工作负载整合等技术提升了运行资源的利用效率,通过关闭空闲资源组件等降低能耗,主要采用多租户共享机制、资源的集中共享可以满足多个客户不同时间段对资源的峰值要求,避免按峰值需求设计容量和性能而造成的资源浪费。资源利用效率的提高可以有效降低运营成本,减少能耗,实现绿色 IT。

(2) 增加业务灵活性

对于使用公共云服务的客户,不需要建设专门的基础设施,缩短业务系统建设周期,使客户能专注于业务的功能和创新,提升业务响应速度和服务质量,实现业务系统的快速部署。对于部署专有云平台的企业,通过云服务供给方式和一键式部署,提高了资源的交付效率,以及业务的灵活性。

(3) 提高业务系统可用性

云计算的资源池化和快速伸缩性特征,使部署在云平台上的客户业务系统可动态扩展,满足业务对 IT 资源的迅速扩充与释放,从而避免因需求突增而导致客户业务系统的异常中断。云平台的备份和多副本机制可提高业务系统的健壮性,避免数据丢失和业务中断。

(4) 提升团队专业性

云计算技术发展迅速,需要有专业技术团队及时更新或采用先进技术和设备,以提供更加专业的技术、管理和人员支撑,使用户能获得更加专业和先进的技术服务。通常只有公共云服务商或大型金融机构具备这些技术能力。

当前我国仍有大量小型或微型金融机构,缺乏完善的基础设施和充足的科技人员,使用公共云服务可以使这些机构在短时间内具备原先只有大机构才能具备的技术能力。

4. 金融业云计算应用现状

目前,在金融业的云计算应用方面,保险业已有全面响应和进展,而银行业、证券业大多广泛在外围应用。

(1) 保险业核心业务系统

由于保监会发布了明确支持云计算的指导文件,因此一些网络保险公司或新兴保险公司已把核心业务系统运行在了具有较高安全保护等级的云平台上。

(2) 非核心系统

对于云计算,金融机构(尤其是银行业金融机构)多数还处于试水的阶段,尚未把核心业务系统和数据库部署到云平台上。大部分金融机构选择采用 X86 服务器搭建云计算平台,将原来承载在主机或小型机上的一些外围应用服务改造为集群化的部署方式,使其不会因硬件故障导致系统运行中断,之后再将改造后的应用服务迁移到云计算平台。而核心系统仍采用相对传统的部署方式。

(3) 互联网业务接入的前置系统

近年来,由于电子商务等互联网相关业务的快速发展,金融机构内部 IT 系统越来越难以支撑相关业务。例如,“双 11”大促销活动,部分金融机构为了支撑“秒杀”类的业务,只能将部分业务压力进行转移,为缓冲系统压力和降低系统风险,金融机构开始将部分网络业务的前置系统转移到云计算平台上来抵消峰值压力,进而从容应对业务的峰值冲击。

(4) 企业互联网网站系统

互联网网站由于技术相对简单、受众覆盖范围广、不涉及太多金融交易,需要高质量的互联网网络平台来提升用户体验,所以一些机构将企业的互联网网站部署在云计算平台。利用云计算平台高质量的网络环境和全方位的地理覆盖,能够为这些机构带来更好的用户体验,同时降低这些机构的互联网带宽需求,节约 IT 运行成本。

(5) 证券业务行情系统

由于证券业务的行情系统只有公开信息,不涉及客户隐私,且对互联网资源要求很高,特别适合使用云计算方式来提供服务。一方面是云平台通常具有很高的带宽,另一方面使用云计算能满足行情淡季和旺季对资源弹性伸缩的需求。

(6) 互联网金融服务系统

互联网金融系统包含微贷、消费金融等相关业务系统。对于互联网金融服务初创企业,由于其系统需要新建,没有历史技术包袱,通过云服务商提供的云服务,可以快速搭建业务系统,降低前期投入,并且天然的互联网业务特性非常适用于云计算相关技术。

(7) 网络学习等辅助系统

企业的网络学习系统是企业内部员工的培训系统,要通过互联网进行访问,并不涉及金融业务,安全等级要求较低,但对用户和系统性能要求较高。因此,部分金融机构将此类系统部署在云平台,不仅提高了系统管理灵活性,降低了运营成本,还大幅改善了用户体验。

(8) 企业开发测试环境

一些金融机构(尤其是银行业金融机构)在试水云计算时,早期仅仅把云计算系统用于开发测试环境,进行应用系统的开发和测试。通过云计算平台的搭建,这些机构的 IT 部门开始逐步体会到云计算平台实现 IT 资源服务化的好处,能够大幅降低系统环境准备的时间和应用上线周期,使得整个开发测试过程更为敏捷。

3.3 区块链技术

3.3.1 区块链概述

1. 区块链概念

区块链(blockchain)技术是指通过去中心化和去信任的方式集体维护一个可靠分布式共享数据库(数据分布式存储和记录)的技术方案,是构建去中心化可信环境的基础协议。该方

案让参与到系统中的任意个节点,把一定时间内系统所有价值交换活动的数据,通过密码学方法计算和记录到一个数据块(即区块 block)中,并生成该数据块的“密码”用于验证其信息的有效性和链接(chain)下一个数据块。

区块链的实质是由多方参与共同维护一个持续增长的分布式账本(Distributed Ledger),其核心是通过分布式网络、时序不可篡改的密码学账本及分布式共识机制,建立彼此之间的信任关系。利用由自动化脚本代码组成的智能合约来编程和操作数据,最终实现由信息互联向价值互联的进化,如图 3-12 所示为传统的中心化账本示意,图 3-13 所示为区块链的去中心化账本示意。



图 3-12 中心化账本

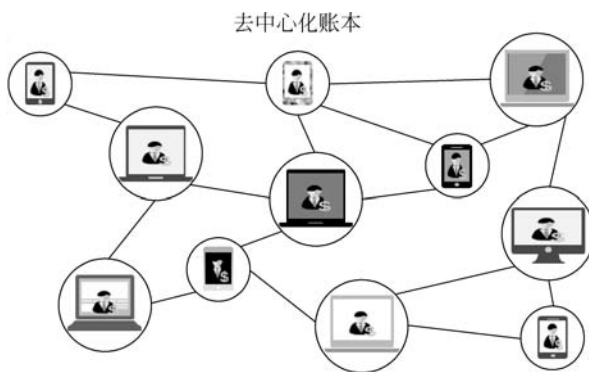


图 3-13 去中心化账本

2. 区块链特点

(1) 去中心化

区块链技术不依赖额外的第三方管理机构或硬件设施,它构建在分布式网络基础上,网络中没有中心化的物理节点和管理机构。通过分布式核算和存储,各个节点实现了信息自我验证、传递和管理网络功能,去中心化是区块链最突出、最本质的特征。

(2) 去信任中介

区块链采用基于协商一致的规范和协议,通过数学原理和公开透明的算法,使得整个系统中的所有节点能够在去信任的环境自由安全地交换数据,实现交易双方在不需要借助第三方权威机构(如中央银行等)信用背书下,通过达成共识建立信任关系。

(3) 共同维护

区块链的维护依赖于网络中所有具有维护功能的节点完成,各个节点的地位是平等的,一个节点甚至几个节点的损坏不会影响整个系统的运作。另外,区块链系统采用特定的经济激励机制来保证分布式系统中所有节点均可参与数据块的验证过程(如比特币的“挖矿”过程),并通过共识算法来选择特定的节点,将新的数据块添加到区块链中。

(4) 开放性

区块链技术基础是开源的,除了交易各方的私有信息被加密外,区块链的数据对所有人都是开放的,任何人都可以通过公开的接口查询、验证区块链共享账本(所有参与者看到的是同一账本)里的每一笔交易数据,因此整个系统信息高度透明。

(5) 时序性

区块链采用带有时间戳的链式区块结构存储数据,具有极强的可追溯性和可验证性。系统中每一个节点都拥有最新的完整数据库副本,一旦信息经过验证添加到区块链上,就会永久

存储。

(6) 安全性

区块链技术采用非对称加密算法对数据进行加密,同时借助分布式系统中各节点的工作量证明等共识算法形成的强大计算能力来抵御外部攻击,保证区块链数据不可篡改和不可伪造,只要不能掌控全部数据节点的 51%,就无法随意操控修改网络数据,这使区块链本身变得相对安全,避免了主观人为的数据变更。

(7) 匿名性

除非有法律规范要求,单从技术上来讲,各区块节点的身份信息不需要公开或验证,信息传递可以匿名进行。

(8) 应用广

区块链技术可以提供灵活的脚本代码系统,支持用户创建高级的智能合约、数字货币或其他去中心化应用。

区块链系统与传统的中心化系统相比有着显著的优势,如表 3-1 所示。

表 3-1 区块链系统与传统中心化系统比较

评判角度	中心化系统	区块链系统	(区块链系统) 特性说明
中心化程度	极高	极低	不依赖第三方,通过自身分布式节点进行网络数据的存储、验证与传递
数据可靠性	中	高	验证结果是过半数节点公认的结果,不会因少数节点被恶意篡改而受到影响
安全性	中	高	单一节点的损坏或失去都不会影响整个系统的运作
信任依赖度	高	极低	参与到系统中的各个节点之间进行数据交换是无须互相信任的
透明度	低	极高	整个系统的运作规则是透明的,数据内容也是公开的
维护成本	较高	低	系统中的数据块由整个系统中所有具有维护功能的节点共同维护,每一个节点在参与记录的同时也验证其他节点记录结果的正确性

3. 区块链分类

按照应用场景和设计体系,可以将区块链分为三类:公有区块链、行业(联盟、联合)区块链和私有区块链,如图 3-14 所示。

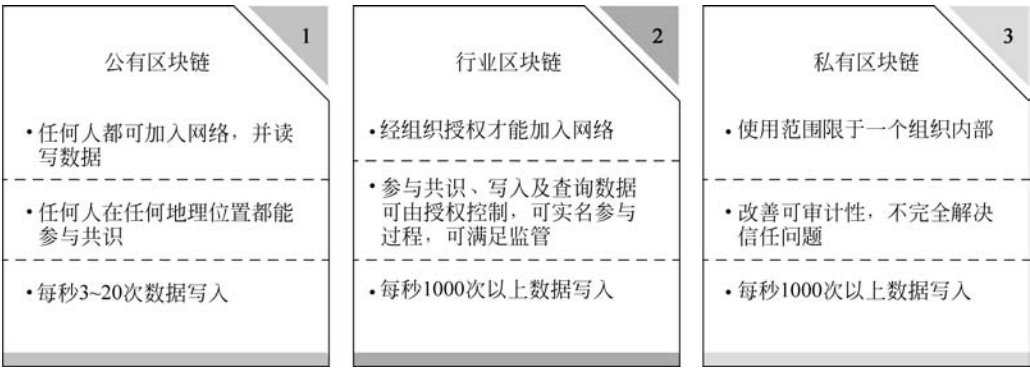


图 3-14 区块链分类

(1) 公有区块链

公有区块链(Public Block Chains)是指世界上任何个体或者团体都可以发送交易,且交易能够获得该区块链的有效确认,任何人都可以参与其共识过程。公有区块链是最早的区块链,也是应用最广泛的区块链,以比特币为代表的主流虚拟数字货币均基于公有区块链,世界上仅有一条该币种对应的区块链。公有链的各个节点可以自由加入和退出网络,并参与对链上数据的读写,读写数据时以扁平的拓扑结构互联互通,网络中不存在任何中心化的服务端节点。

(2) 行业(联盟、联合)区块链

行业区块链(Consortium Block Chains)的各个节点通常有与之对应的实体组织和机构,只有通过授权才能加入与退出网络。行业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,预选节点的多少,如何决定每个块的记账者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。由此,行业区块链各组织和机构组成利益相关的联盟,共同维护区块链的健康运转。

(3) 私有区块链

私有区块链(Private Block Chains)仅仅使用区块链的总账技术进行记账,可以是一个公司,也可以是个人,独享该区块链的写入权限。私有区块链与其他的分布式存储方案没有太大区别。私有区块链的各个节点的写入权限由组织内部控制,而读取权限可视需求有选择性地对外开放。私有区块链仍然具备区块链多节点运行的通用结构,适用于特定组织和机构的内部数据管理与审计。

4. 区块链的发展

许多人都会把区块链的发展历史与比特币的发展历史相混淆,实际上比特币只是区块链的一个较为成熟的应用,区块链还应用于其他许多领域。区块链的发展经历了两个阶段,第一个阶段为理论阶段,第二个阶段为应用阶段。

小资料 3-2

拜占庭将军问题的由来

拜占庭将军问题(Byzantine Failures)是由莱斯利·兰伯特提出的点对点通信中的基本问题。含义是在存在消息丢失的不可靠信道上,试图通过消息传递的方式达到一致性是不可能的。因此,对一致性的研究一般假设信道是可靠的或不存在该问题。

拜占庭将军问题的起源

拜占庭位于如今土耳其的伊斯坦布尔,是古代东罗马帝国的首都。由于当时拜占庭罗马帝国国土辽阔,为了达到防御目的,每个军队都分隔很远,将军与将军之间只能靠信差传递消息。在战争的时候,拜占庭军队内所有将军和副官必须达成一致的共识,决定是否赢的机会才去攻打敌人的阵营。但是,在军队内有可能存有叛徒和敌军的间谍,左右将军们的决定又扰乱整体军队的秩序。在形成共识时,结果并不代表大多数人的意见。这时候,在已知有成员谋反的情况下,其余忠诚的将军在不受叛徒的影响下如何达成一致的协议,拜占庭问题就此形成。

拜占庭将军的问题

拜占庭将军问题是一个协议问题,拜占庭帝国军队的将军们必须全体一致决定是否攻击某一支敌军。问题是这些将军在地理上是分隔开来的,并且在将军中存在叛徒。叛徒可以任意行动以达到以下目标:欺骗某些将军采取进攻行动;促成一个不是所有将军都同意的决定,如当将军们不希望进攻时促成进攻行动;或者迷惑某些将军,使他们无法做出决定。如果叛徒达到了这些目的之一,则任何攻击行动的结果都是注定要失败的,只有完全达成一致的努力才能获得胜利。

拜占庭假设是对现实世界的模型化,由于硬件错误、网络拥塞或断开以及遭到恶意攻击,计算机和网络可能出现不可预料的行为。拜占庭容错协议必须处理这些失效,并且这些协议还要满足所要解决问题要求的规范。

1) 理论阶段

区块链的理论阶段,其实就是密码学和货币理论的发展和完善阶段。

1976年,迪菲(Bailey W. Diffe)和赫尔曼(Martin E. Hellman)两位密码学大师发表了论文《密码学的新方向》,这篇论文覆盖了密码学所有的新进展,包括非对称加密算法、椭圆曲线加密算法、散列算法等,奠定了迄今为止整个密码学发展的方向,也对区块链的技术和比特币的诞生起到决定性作用。同一年,哈耶克出版了《货币的非国家化》,这本书所提出的非主权货币、竞争发行货币等理念,可以说是去中心化货币的精神指南。

1976年是作为区块链理论发展的元年,正式开启了整个密码学,包括密码学货币的时代。

紧接着在1977年,著名的RSA算法诞生,这是1976年《密码学的新方向》的自然延续,该算法的三位发明人也因此获得了2002年的图灵奖。

1980年,Merkle Ralf提出了默克尔树(Merkle-Tree)结构和相应的算法,其主要用于对分布式网络中数据同步的正确性进行检验,也是比特币中进行区块同步检验的重要手段。

1982年,Lamport提出了拜占庭将军问题,标志着分布式计算的可靠性理论和实践进入实质性阶段。同年,大卫·乔姆提出了密码学支付系统eCash。可以看出,随着密码学的进展,人们已经开始将其运用到货币、支付等相关领域中。可以说,eCash是密码学货币的先驱之一。

1985年,Koblitz和Miller各自独立提出了著名的椭圆曲线加密(Elliptic Curve Cryptography, ECC)算法。由于此前发明的RSA算法计算量过大,且难以实用,而椭圆曲线加密算法的提出使得非对称加密体系真正走向实用渠道。因此,1985年,也就是《密码学的新方向》发表10年左右的时候,现代密码学的理论和技术基础就已经完全确立了。

1997年,HashCash方法——也就是第一代工作量证明(Proof of Work, PoW)算法出现了,这种方法在当时主要用于反垃圾邮件。

到了1998年,密码学货币的完整思想终于破茧而出,戴伟(Wei Dai)、尼克·萨博(Nick Szabo)同时提出密码学货币的概念。其中,戴伟的B-Money称为比特币的精神先驱,而尼克·萨博的BitGold提纲与比特币开发者兼创始者中本聪提出的比特币特性非常接近。

在21世纪到来之际,区块链领域又有了几次重大的进展:首先是点对点(peer to peer, P2P)网络出现(如: Napster、eDonkey2000、BitTorrent),奠定了P2P网络计算的基础;其次,是2001年美国国家安全局(NSA)发布了SHA-2系列算法,其中就包括目前应用最广的

SHA-256 算法,这也是比特币最终所采用的散列算法。可以说,到了 2001 年,比特币或者区块链技术诞生的所有技术基础在理论和实践上都被解决了,比特币呼之欲出。

2) 应用阶段

区块链理论成熟之后,中本聪于 2008 年 11 月发表了著名的论文《比特币:一种点对点的电子现金系统》,并于 2009 年 1 月用他的第 1 版软件挖掘出了创世区块,这个区块中包含着这样一句话:“The Times 03/Jan/2009 Chancellor on brink of second bailout for banks”,标志着区块链进入应用阶段。这个阶段的区块链在应用层面形成了区块链 1.0、区块链 2.0 和区块链 3.0 的概念。

(1) 区块链 1.0

区块链 1.0 就是以比特币为代表的虚拟货币,它虽然问题重重,包括价格的剧烈波动、数量上限可能导致的通货紧缩、挖矿对能源的浪费、各国政府监管的限制等,但其仍然是区块链技术最成功的应用,并为人们勾勒了一幅理想的远景图——全球货币的统一和货币的发行不再仅仅依赖于各国的中央银行。区块链 1.0 的起点很高,但路途可能是最遥远的,因为要连起这样一个全球的区块链网络,需要所有个人和机构的共同参与。

(2) 区块链 2.0

区块链 2.0 可以被理解为区块链技术在其他金融领域的运用,包括华尔街各家银行联合起来打造区块链行业标准,提高银行结算支付效率,降低跨境支付成本;交易所积极尝试用区块链技术实现股权登记、转让等功能。

(3) 区块链 3.0

区块链 3.0 将区块链应用的领域扩展到金融行业之外,覆盖了人类社会生活的方方面面。在各类社会活动中实现信息的自证明,不再依靠某个第三方获得信任或建立信用;实现信息在司法、医疗、物流等各个领域的共享,利用区块链技术解决信任问题,提高整个系统的运转效率。

3) 区块链的发展现状

(1) 我国区块链的发展现状

区块链由于其所具有的高性能、高安全性、高速接入、高效运营等优势引起了人们的广泛关注。在区块链迅速发展的背景下,我国顺应全球化需求,紧跟国际上区块链的研究前沿,积极推动境内区块链的相关领域研究、标准化制定以及产业化发展。

2015 年 12 月,中国区块链研究联盟、中国区块链应用研究中心成立;2016 年 2 月,中关村区块链产业联盟成立;2016 年 2 月,时任中国人民银行行长的周小川先生指出,数字货币必须由中央银行发行,区块链是一项可选的技术;2016 年 4 月,中国分布式总账基础协议联盟(Chinaledger)宣布成立;2017 年 2 月,中国人民银行基于区块链的数字票据交易平台测试成功。由此,我国区块链标准和技术不断完善,应用场景也由金融支付拓展到其他服务领域。

目前,我国区块链政策日益明晰,主要的行业政策指导文件有 2016 年 10 月国家工业和信息化部发布的《中国区块链技术和应用发展白皮书》、2016 年 12 月国务院发布的《“十三五”国家信息化规划》以及 2017 年 5 月 16 日工业和信息化部发布的《区块链参考架构》。

2016 年,国际标准化组织(ISO)成立了专注于区块链的技术委员会 ISO/TC307(区块链与分布式记账技术标准化技术委员会),开展基础、身份认证、智能合约等重点方向的标准化工作。我国以参与国(P 成员)身份参加了相关的标准化活动,取得了积极的进展。为尽快推动形成完备的区块链标准体系,做好 ISO/TC307 技术对口工作,2018 年工业和信息化部信息化

和软件服务业司指导中国电子技术标准化研究院提出全国区块链和分布式记账技术标准化技术委员会组建方案。

(2) 国际区块链的发展现状

随着区块链的快速发展,其优势和特性逐渐体现,区块链的全球化进程开始向前迈进。

2015年,部分国家认识到区块链技术的巨大应用前景,开始从国家发展层面考虑区块链的发展道路,“区块链”成为全球各大监管机构、金融机构及商业机构争相研究和讨论的对象。从整体上看,各大金融机构普遍对区块链技术在改善其后端流程效率以及降低运作成本的可能性上有着较为积极的态度。部分国家政府一改过去持有的对比特币的反对态度,转而积极推动区块链技术和应用的发展。区块链开始在各国迅速发展,可以通过各国区块链相关政策的对比看出端倪。如表3-2所示。

表 3-2 各国区块链政策发展

国家或地区	政策发展
俄罗斯	2014年,俄罗斯财政部建议禁止比特币及加密电子货币的操作;2016年初,中央银行考虑比特币合法化和交易监管,尤其是P2P交易及个人业务托管;2017年1月,将关于“合法化”区块链技术的发展路线图提交给总统批准
美国	2015年1月,批准比特币交易所成立,比特币监管立法初步完成;2015年6月,数字货币公司监管框架最终版本BitLicense发布,多家监管机构表明支持区块链技术发展;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,推动政府数据分析、连接设备和区块链的研究发展
日本	2016年5月,日本首次批准数字货币监管法案,并将其定义为财产;成立首个区块链行业组织——区块链合作联盟(BCCC)
韩国	2015年年底,新韩银行参与区块链企业融资;2016年2月,中央银行在报告中提出鼓励探索区块链技术;同月,证券交易所(KRX)宣布正在开发基于区块链技术的交易平台
德国	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存储
英国	2016年1月,发布白皮书《分布式账本技术:超越区块链》,第一次从国家层面对区块链技术的未来发展和应用进行了全面分析,并给出研究建议;2016年6月,进行区块链试点,跟踪福利基金的分配以及使用情况
欧盟	2016年2月,欧盟委员会将加密数字货币放在快速发展目标领域的首位,推动各机构对数字货币的政策研究;2016年4月,欧洲数字货币与区块链技术论坛(EDCAB)举办集中讨论区块链的“博览会”;中央银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
加拿大	2016年6月,中央银行展示了利用区块链技术开发的CAD-Coin,即电子版加元
澳大利亚	2015年年底,证券交易所(ASX)考虑申请区块链技术以提高其交易系统,作为其清算和结算系统的替代品;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;新政党Flux正在试图利用区块链技术改写政治通货制度

3.3.2 区块链原理

区块链技术原理的来源可以归纳为前面提到过的一个数学问题,即拜占庭将军问题。将拜占庭将军问题延伸到互联网生活中来,其内涵可以概括为:在互联网大背景下,当需要与不熟悉的手进行价值交换活动时,人们如何防止不会被其中的恶意破坏者欺骗、迷惑,从而做出错误的决策。若将拜占庭将军问题进一步延伸到技术领域中来,其内涵可以概括为:在缺

少可信任的中央节点和可信任的通道情况下,分布在网络中的各个节点应如何达成共识。区块链技术有效解决了著名的拜占庭将军问题——它提供了一种无须信任单个节点,还能创建共识网络的方法。

1. 区块链技术解决的问题

有学者把区块链用四个字概况为“记账”和“认账”。也就是说,区块链技术解决的问题就是如何记账和如何认账。

1) 记账方式——分布式

记账就要有一个账本。区块链就是一个网络大账本,每个人都有权在上面记账。但这个账本与传统的账本不一样,记账方式也和传统的会计记账方式不一样。区块链根据系统确定的开源的、去中心化的协议,构建了一个分布式结构的记账体系,它由分布式记账、分布式传播和分布式存储3部分构成,如图3-15所示。



图 3-15 区块链的记账方式

(1) 分布式记账

分布式记账——会计责任的分散化(Distributed Account Ability)。

区块链设计者没有为专业的会计记账员预留一个特定的位置,而是采用分布式记账方式,交易记账由分布在不同地方的多个节点共同完成,而且每一个节点记录的是完整的账目。通俗地说,区块链技术就是一种全民参与记账的方式。

(2) 分布式传播

区块链依靠点对点网络系统,每次交易都会对网络里所有的参与者进行广播,并且经过多次确认后才被记录到区块链分布式账本中。而传统的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。

(3) 分布式存储

区块链采取分布式存储方式存储账本,但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:一是分布,分布在区块链每个节点的数据都按照区块链式结构存储的完整数据(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分布存储,分布存储在每个节点上的数据仅是其中一份);二是去中心化,区块链每个节点存储都是独立的、地位等同的,并且依靠共识机制保证存储的一致性。

由于区块链上没有任何一个节点可以单独记录账本数据,从而避免了单一记账人被控制或者被贿赂而假记账的可能性。当记账节点足够多时,理论上讲,除非所有的节点被破坏,否则账目就不会丢失,从而保证了账目数据的安全性。

2) 认账方式——“去中心化+共识”机制

区块链是一种利用“去中心化”的“信任(共识)”机制,集体维护一组数据库账簿的可靠性技术方案,是一个可信的数据库,可靠的“账本”。即区块链认账方式是通过“去中心化”机制和“共识”机制实现的。

(1) 去中心化机制

区块链上每一个参与者都会有自己的账本,每一个节点都是平等的,不存在中心化的管理机构,这种“去中心化”的特点使得区块链无须依赖第三方,其运作不需要任何人为干预,能够独立地进行自我验证。

举个例子,过去李四要向张三借 10 元钱,需要找王二做信用担保,同时要找专业的赵一来记账,如果有人修改了赵一的账本,所有的记账便乱套了。而有了区块链技术,当李四要向张三借钱的时候,只要在群里通知到所有人,并且当大家都在各自的账本上记录李四欠张三 10 元钱时,这笔交易便完成了。这个系统中不需要银行,也不需要借贷协议和收据。这便是区块链的“去中心(中介)化”机制。

(2) 共识机制

共识机制就是所有记账节点之间怎么达成共识,去认定一个记录的有效性,这既是认定的手段,也是防止篡改的手段。一旦信息被记录,就会被永久储存且永远不能被更改。比如上面例子中,李四突然改口说:“我不欠张三的钱”,这个时候区块链上所有参与者都会为张三作证,如图 3-16 所示。

区块链上所有信息都是共享的、透明的,做不了假账,极大地降低了风险,使得黑客无从下手。当虚假信息发生时,区块链可以通过相互对证来破除,从而保证网络安全。这便是区块链的“共识”机制。



图 3-16 区块链的“共识”机制

供应链金融是区块链技术落地金融的最佳场景。传统的供应链金融是一种中心化模式,基本上都是金融机构、保理公司依托一家核心企业,来为供应链上超过 80% 的中小企业提供服务,因为所有的交易最终都需要核心企业的“确权”,这使得核心企业权力太大,造成信息的不透明,这不仅严重影响整个链条的效率,也不利于构建供应链信用体系,如图 3-17 所示。

区块链技术可帮助中小企业累积信息数据,能更准确地评价企业的真实经营状况,低成本高效率地做出放贷决策。在供应链条上,供应商、核心企业、银行、金融机构等多方并存的交易场景最适合应用区块链技术。运用区块链技术,可以为应收账款、票据、仓单等资产确权,减少中间环节,并且留下数据存证,防止票据作假、重复质押等风险的发生。

小资料 3-3

金融术语——保理

保理(Factoring)全称保付代理,又称托收保付,是一个金融术语,指卖方将其现在或将来的基于其与买方订立的货物销售/服务合同所产生的应收账款转让给保理商(提供保理

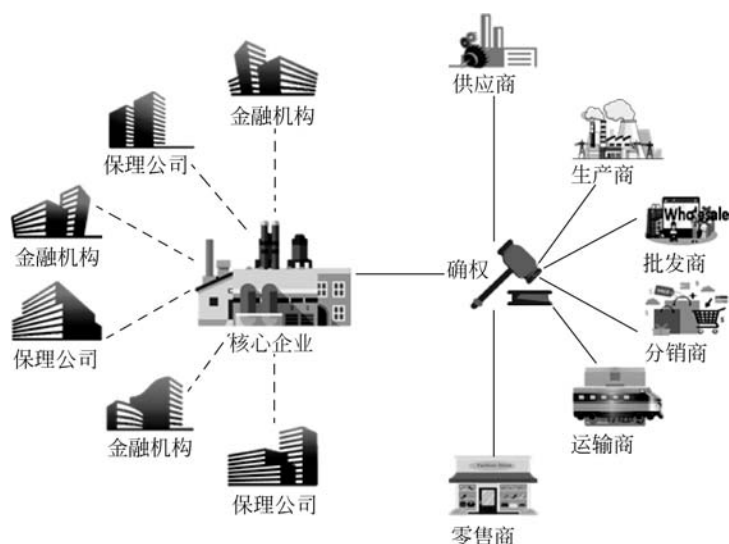


图 3-17 传统的供应链金融

服务的金融机构),由保理商向其提供资金融通、买方资信评估、销售账户管理、信用风险担保、账款催收等一系列服务的综合金融服务方式。它是商业贸易中以托收、赊账方式结算货款时,卖方为了强化应收账款管理、增强流动性而采用的一种委托第三者(保理商)管理应收账款的行为。

保理业务的分类:商业保理,指由非银行保理商开展的保理业务;国内保理,指保理商为在国内贸易中的买方、卖方提供的保理业务;国际保理,指保理商为在国际贸易中的买方、卖方提供的保理业务。还可以按照保理商是否承担债务人的信用风险分类,可分为有追索权保理和无追索权保理。

(资料来源:百度百科)

例如,一家汽车制造商,向 A 企业订购一批车门,但 A 企业不能完全自己生产,它要再去找其他供应商订购配件,但是在传统的供应链金融领域,只承认 A 企业,而 A 企业的供应商们,却无法获得供应链金融服务。区块链介入后,汽车制造商发了 1000 万个信用 token,只要下游的供应商拿到 token,就证明与核心企业有合作,这就变相做到了“资产穿透”,如图 3-18 所示。

其实业界对区块链的使用有三点共识:一是实现数据信任;二是简化流程,提高效率,降低交易对手信用风险;三是提升透明度和监管效率,避免欺诈行为。

正是区块链这种革命性的“记账”与“认账”模式,使得澳大利亚证券交易所率先引入区块链技术进行股票交易;北爱尔兰银行积极推行数字货币发行;美国白宫斥巨资引入区块链技术;纳斯达克公开发行了首只区块链技术股票。假如未来区块链普及,人们就不用再去银行证明个人收入和资产,不用去派出所证明是否已婚,也不用再去相关部位加盖各种证明印章。而所有这些都记录在不可篡改的区块链上,在我们需要授权的时候,全世界都能成为我们的证人。

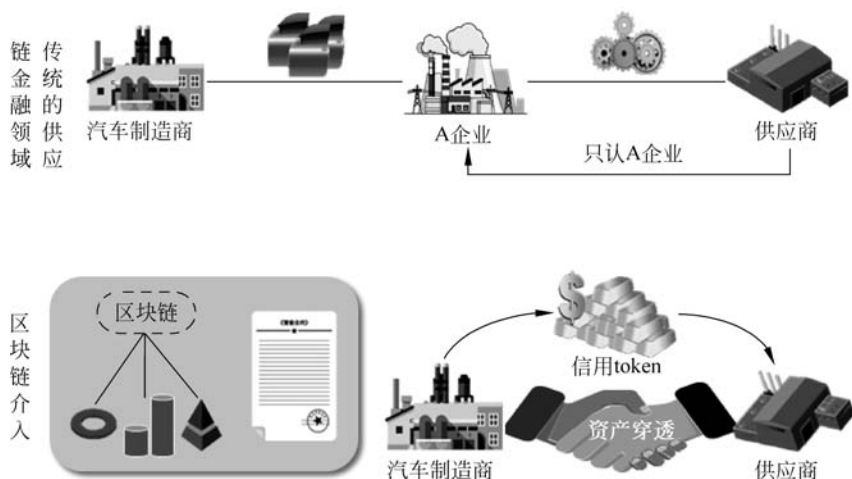


图 3-18 传统的供应链金融与区块链供应链金融

2. 区块链的核心技术

1) 核心技术一：“区块+链”式数据结构

区块链的数据结构是“区块+链”的结构,即区块链把数据分成不同的区块,每个区块通过特定的信息链接到上一个区块的后面,这些区块前后顺连来呈现一套完整的数据。

(1) 区块

在区块链技术中,数据以电子记录的形式被永久地存储下来,存放这些电子记录的文件就称为“区块”。区块是按时间顺序一个一个先后生成的,每一个区块记录了它在被创建期间发生的所有价值交换数据(交易数据),所有区块汇总起来形成一个记录合集。

(2) 区块结构

区块中会记录下区块生成时间段内的交易数据,区块主体实际上就是交易数据的合集。各种区块链的结构设计可能不完全相同,但在结构上都大体分为块头(header)和块身(body)两部分。块头用于链接到前面的区块并为区块链数据库提供完整性的保证,块身则包含了经过验证的、区块创建过程中发生的价值交换的所有记录。

区块结构有两个重要的特点:第一,每一个区块上记录的交易数据是上一个区块形成之后和该区块被创建之前发生的所有价值交换活动,这个特点保证了数据库的完整性。第二,在绝大多数情况下,一旦新的区块完成并被加入区块链的最后,则此区块的记录就再也不能被改变或删除。这个特点保证了数据库的严谨性,即无法被篡改。

(3) 区块链

区块链就是区块以链的方式组合在一起,以这种方式形成的数据库为区块链数据库,如图 3-19。

(4) 区块链的基本结构

区块链是系统内所有节点共享的交易数据库,这些节点基于价值交换协议参与到区块链的网络中来。那么区块链是如何做到这些的呢?由于每一个区块的块头都包含了前一个区块的交易数据压缩(交易缩影)值,这就使得从创世块(第一个区块)到当前区块的各个区块链接在一起,形成了一条长链。如果不知道前一个区块的“交易缩影”值,就无法生成当前区块,因此每个区块必定是按时间顺序链接在前一个区块之后。这种所有区块都包含前一个区块引用

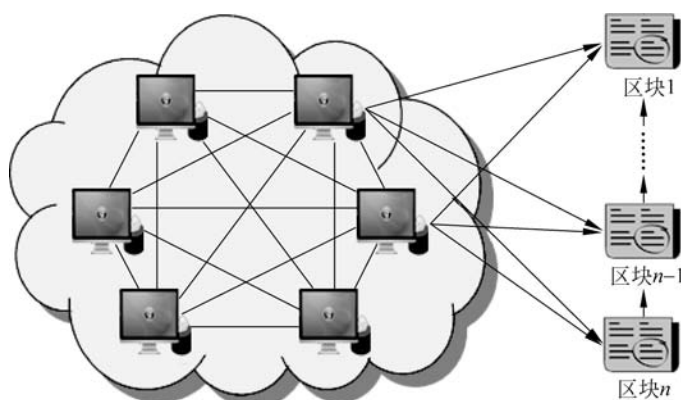


图 3-19 区块链数据库

的结构让现存的区块集合形成了一条数据长链。

区块链的基本结构可以总结如下：人们把一段时间内生成的信息(包括数据或代码)打包成一个区块，盖上时间戳，与上一个区块衔接在一起，每一个区块的页首都包含了上一个区块的索引数据，然后再在本页中写入新的信息，从而形成新的区块，首尾相连，最终形成了区块链。这个结构的核心思想是：区块(完整历史)+链(完全验证)=时间戳，如图 3-20 所示。

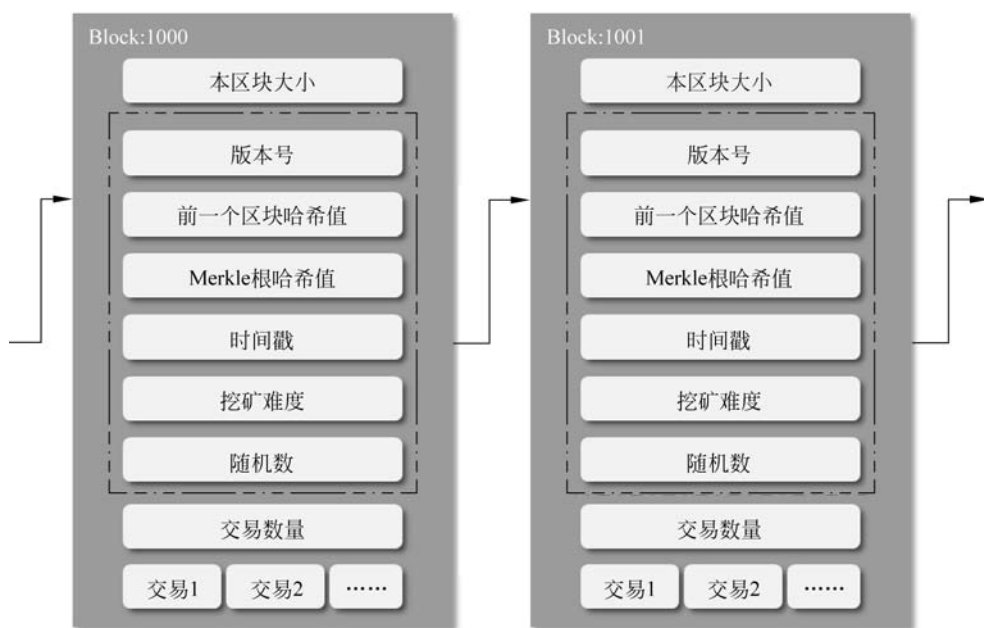


图 3-20 区块与区块链

“区块+链”的结构为人们提供了一个数据库的完整历史。从第一个区块开始，到最新产生的区块为止，区块链上存储了系统全部的历史数据。

区块链提供了对数据库中每一条交易数据的查找功能。区块链上的每一条交易数据，都可以通过“区块链”的结构追本溯源，逐一进行验证。

区块+链=时间戳，这是区块链数据库的最大创新点。区块链数据库让整个网络的记录者在每一个区块中都通过盖上一个时间戳来记账，表示这个信息是这个时间写入的，从而形成

了一个不可篡改、不可伪造的数据库。

2) 核心技术二：分布式账本——开源的、去中心化的协议

区块链根据开源的、去中心化的协议来解决记录(记账)和存储(认账)的问题。具体实施步骤如下。

(1) 记录数据(记账)

区块链对于这个问题的处理办法是构建一整套协议机制,让网络中的每一个节点都在参与记录的同时也去验证其他节点记录结果的正确性。只有当网络中的大部分节点(甚至所有节点)都同时认为这个记录正确,或者所有参与记录的节点都对结果一致通过时,记录的真实性才能得到整个网络的认可,记录数据也才被允许写入区块。

(2) 存储数据(认账)

区块链对于这个问题的处理办法是构建一个具有分布式结构的网络,对于数据库中的所有数据都实时更新并将它们存放于所有参与记录的网络节点中。这样即使部分节点损坏或被黑客攻击,也不会影响整个数据库的数据记录与信息更新。

通过这种方式记录和存储的价值交换数据再通过分布式传播发送给整个网络,实现分布式存储。

通过分布式传播、分布式记账、分布式存储这三大分布式技术可以发现,没有任何个人、组织、甚至国家能够控制这个系统,系统内的数据存储、交易验证、信息传输过程都是去中心化的。在没有中心的情况下,大规模的参与者达成共识,共同构建了区块链数据库。可以说,这是人类历史上第一次构建了一个真正意义上的去中心化体系。甚至可以说,区块链技术构建了一套永生不灭的系统——只要网络中的所有参与节点没有在同一时间集体崩溃,数据库系统就可以一直运转下去。

3) 核心技术三：非对称加密

有了一个严谨的数据库,接下来就是如何使这个严谨且完整存储下来的数据库变得可信赖,使得人们可以在互联网无实名的背景下成功防止诈骗。事实上,区块链还有一个优点就是隐蔽性。除了保护私人信息,在信息交互过程中各参与方的身份也是匿名的。也就是说,当你查看某个数据时,你并不知道这个数据是谁做的,而对方也无法知道是你看了这些数据。因此,区块链被认为是有史以来最安全的数据管理方式。区块链系统解决这一问题采用的技术是非对称加密。非对称加密是一种保证区块链安全的基础技术,也是区块链核心技术之一。

非对称加密用两个数学相关的数字密钥对信息进行编码。其中一把为公钥,公钥用加密算法来加密信息;另一把作为私钥用来解密收到的信息。也就是说,用作公钥和私钥的两把钥匙,如果一把用于加密,另一把就可用于解密。

非对称加密系统有两种基本应用模式:加密模式和验证模式。

(1) 加密模式

在加密模式中,非对称加密系统对信息的加密和解密过程如图 3-21 所示。

在发送端 A,首先发送方 A 用接收方 B 的公开密钥 K_{pb} 对要发送的原文进行加密;然后将加密后的密文通过网络传送给接收方 B。在接收端 B,接收方 B 用自己的私有密钥 K_{sb} 对接收到的密文进行解密,就得到了发送端发来的原文。

在加密模式中,加密是用指定的接收方 B 的公钥加密,所以只有指定的接收方 B 才能解开密文,因为私有密钥是在指定的接收方手中。

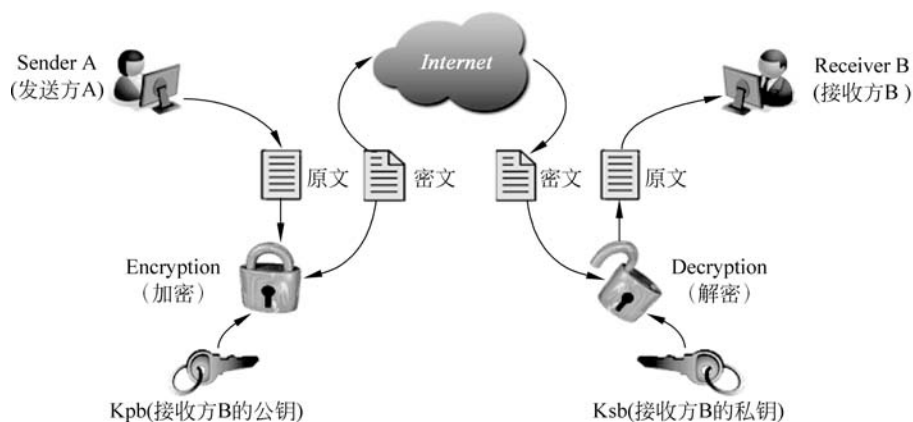


图 3-21 非对称加密系统的加密模式

(2) 验证模式

非对称加密技术不但可以用于加密以确保信息的隐蔽性,还可以用于验证模式,来确保信息的完整性、不可否认性和真实性。

在验证模式中,非对称加密系统对信息的加密和解密过程如图 3-22 所示。

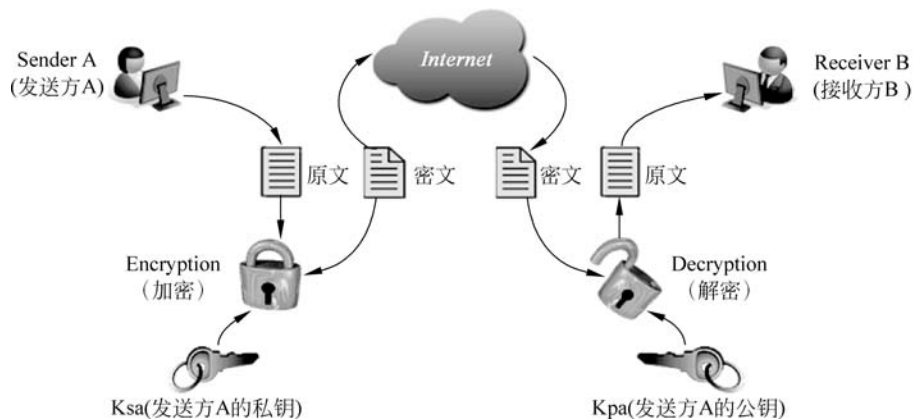


图 3-22 非对称加密系统的验证模式

在发送端 A,首先发送方 A 用自己的私有密钥 K_{sa} 对要发送的原文进行加密;然后发送方 A 将加密后的密文通过网络传送给接收方 B。在接收端 B,接收方 B 用发送方 A 的公开密钥 K_{pa} 对接收到的密文进行解密,最后得到原文。

在验证模式中,任何能够成功地解密接收到密文的接收方,都能肯定该消息确实是来自发送方,因为只有发送方才拥有与解密公钥相对应的加密私钥,从而验证了该信息确实来自发送方。也就是说,在验证模式中,任何接收者都可以用发送方的公钥解密发送方发来的信息,从而验证信息是发送方发来的;但是任何人都不能伪造发送方发送信息。

从信任的角度来看,区块链实际上是用数学方法解决信任问题。在区块链技术中,所有的规则都事先以算法程序的形式表述出来,人们完全不需要知道交易的对方是“君子”还是“小人”,更不要求助于中心化的第三方机构来进行交易背书,而只需要信任数学算法就可以建立互信。区块链技术的背后,实质上是数学算法在为人们创造信用、达成共识背书。

4) 核心技术四: 智能合约

智能合约(Smart Contract)是一种旨在以信息化方式传播、验证或执行合同的计算机协议,它允许在没有第三方的情况下进行可信交易,这些交易可追踪且不可逆转。

在区块链中,智能合约就是一段可编程的脚本,它基于可信的不可篡改的数据,自动化地执行一些预先定义好的规则和条款。在若干笔交易中,只要叠加了“智能合约”,所有的交易达到条件后就可自动执行。

区块链中的智能合约继承了区块链的3个特征:数据透明、不可篡改、永久运行。

3. 区块链的共识机制类型

区块链作为一种按时间顺序存储数据的数据结构,可支持不同的共识机制。共识机制是区块链技术的重要组件。区块链共识机制的目标是使所有的诚实节点保存一致的区块链视图,同时满足两个性质:一是一致性,所有诚实节点保存的区块链前缀部分完全相同;二是有效性,由某诚实节点发布的信息终将被其他所有诚实节点记录在自己的区块链中。

目前区块链的共识机制主要有以下五种。

(1) 工作量证明(Proof of Work, PoW)

工作量证明机制即对于工作量的证明,用一句话介绍:干得越多,收获越多。依赖机器进行数学运算来获取记账权,是生成要加入区块链中的一笔新的交易信息(即新区块)时必须满足的要求。在基于工作量证明机制构建的区块链网络中,节点通过计算随机哈希散列的数值解争夺记账权,求得正确的数值解以生成区块的能力是节点算力的具体表现。工作量证明机制具有完全去中心化的优点,在以工作量证明机制为共识的区块链中,节点可以自由进出。比特币网络就是应用工作量证明机制来生产新的货币。然而,由于工作量证明机制在比特币网络中的应用已经吸引了全球计算机大部分的算力,其他想尝试使用该机制的区块链应用很难再获得同样规模的算力来维持自身的安全。同时,基于工作量证明机制的挖矿行为还造成了大量的资源浪费,达成共识所需要的周期也较长。也就是说,工作量证明机制的资源消耗相比其他共识机制高、可监管性弱,同时每次达成共识,需要全网共同参与运算,性能效率比较低,容错性方面允许全网50%节点出错。因此该机制并不适合商业应用。

优点:

- ① 算法简单,容易实现。
- ② 节点间无须交换额外的信息即可达成共识。
- ③ 破坏系统需要投入极大的成本。

缺点:

- ① 消耗大量能源。
- ② 区块的确认时间难以缩短。
- ③ 新的区块链必须找到一种不同的散列算法,否则就会面临比特币的算力攻击。
- ④ 需要等待多个确认,容易产生分叉。

(2) 权益证明(Proof of Stake, PoS)

权益证明机制是工作量证明机制的一种升级共识机制,与要求证明人执行一定量的计算工作不同,权益证明要求证明人提供一定数量加密货币的所有权即可。用一句话概括就是持有越多,获得越多。

权益证明机制的运作方式是,当创建一个新区块时,矿工需要创建一个“币权”交易,交易会按照预先设定的比例把一些币发送给矿工本身。权益证明机制根据每个节点拥有代币的比

例和时间,依据算法等比例降低节点的挖矿难度(主要思想是节点记账权的获得难度与节点持有的权益成反比),从而加快了寻找随机数的速度。这种共识机制相对于 PoW 而言,一定程度上减少了数学运算带来的资源消耗,性能也得到了相应的提升,但本质上仍然需要网络中的节点进行挖矿运算,依然是基于哈希运算竞争获取记账权的方式。因此,PoS 机制并没有从根本上解决 PoW 机制难以应用于商业领域的问题。

优点:在一定程度上缩短了共识达成的时间,不再需要大量消耗能源挖矿。

缺点:还是需要挖矿。所有的确认都只是一个概率上的表达,而不是一个确定性的事情,理论上有可能存在其他攻击影响。

(3) 委托权益证明(Delegated Proof of Stake, DPoS)

与 PoS 原理相同,只是选了一些“代表”。与 PoS 的主要区别在于节点选举若干代理人,由代理人验证和记账。其合规监管、性能、资源消耗和容错性与 PoS 相似。与董事会投票类似,该机制拥有一个内置的实时股权人投票系统,就像系统随时都在召开一个永不散场的股东大会,所有股东都在这里投票决定公司决策。基于 DPoS 机制建立的区块链的去中心化依赖于一定数量的代表,而非全体用户。在这样的区块链中,全体节点投票选举出一定数量的节点代表,由它们来代理全体节点确认区块、维持系统有序运行。同时,区块链中的全体节点具有随时罢免和任命代表的权力。如果必要,全体节点可以通过投票让现任节点代表失去代表资格,重新选举新的代表,实现实时的民主。

优点:大幅度缩小参与验证和记账节点的数量,从而达到秒级的共识验证。

缺点:整个共识机制还是依赖于代币(token),很多商业应用是不需要代币存在的。因此,该共识机制仍然不能完美解决区块链在商业中的应用问题。

(4) 实用拜占庭容错(Practical Byzantine Fault Tolerance, PBFT)

在保证活性和安全性(Liveness & Safety)的前提下提供了 $(N-1)/3$ 的容错性。在分布式计算上,不同的计算机透过信息交换,尝试达成共识;但有时候,系统上协调计算机(Coordinator)或成员计算机(Member)可能因系统错误并交换错误的信息,导致影响最终的系统一致性。

拜占庭将军问题就根据错误计算机的数量,寻找可能的解决办法,这无法找到一个绝对的答案,只可以用来验证一个机制的有效程度。

拜占庭问题的可能解决方法如下。

在 $N \geq 3F + 1$ 的情况下,一致性是可能解决。其中, N 为计算机总数, F 为有问题计算机总数。信息在计算机间互相交换后,各计算机列出所有得到的信息,以大多数的结果作为解决办法。

优点:

① 系统运转可以脱离代币的存在,PBFT 算法共识各节点由业务的参与方或者监管方组成,安全性与稳定性由业务相关方保证。

② 共识的时延为 2~5 秒,基本达到商用实时处理的要求。

③ 共识效率高,可满足高频交易量的需求。

缺点:

① 当有 $1/3$ 或以上记账人停止工作后,系统将无法提供服务。

② 当有 $1/3$ 或以上记账人联合作恶,且其他所有的记账人被恰好分割为两个网络孤岛时,恶意记账人可以使系统出现分叉,但是会留下密码学证据。

小资料 3-4**雅浦岛石币**

雅浦岛是一个位于太平洋、人口不到一万人的小岛。由于当地不出产金属,于是石头便成为当地重要的资源,并发展出以石头充当交易媒介的贸易模式。当地人称这种石币为费。

石币的直径大小不等,小的直径约 30 厘米,大的可以大到直径 3 米(厚约 50 厘米,重达四吨)。石币中间有一个孔,方便插入杆作搬运之用。石币越大,质地越好,该石币所代表的价值便越高。但石币的价值不仅在于它的大小重量或是雕刻工艺上的展现,还包含了运送途中有多么艰难,或这块石币是由某位有名的水手所运送的,像这些背后的故事都可以增加该石币的价值。居民拥有石币的数量和大小代表了财富的多寡。

岛上的居民十分信任石币内含的购买力,当交易所涉及的费用太高时,受石币重量所限,这些石币是不会从前所有者搬运到新的拥有者手上,亦即并不是一手交货,一手交钱的交易,只是在石币上留下标记注明所有者是谁,表示所有权已经易手。只要大家认可这个石币的所有权谁属,便承认了财富的转移。

岛上有一户人家,他祖先曾得一巨大且质地佳的石币,但由于运回雅浦岛的途中遇上海难而石沉大海,但当地的居民仍相信,即便物理上石币已从众人眼前消失,但理论上石币依然存在,只是不在拥有者家中,石币的购买力并不会因为石币所处的地点而有所下降,所以这户人家仍储存了石币代表的价值,得到了该石币所代表的财富。

(资料来源:百度百科)

(5) 授权拜占庭容错(delegated BFT,dBFT)

由权益来选出记账人,然后在记账人之间通过拜占庭容错算法来达成共识。

此算法在 PBFT 基础上进行了以下改进。

- ① 将 C/S 架构的请求响应模式,改进为适合 P2P 网络的对等节点模式。
- ② 将静态的共识参与节点改进为可动态进入、退出的动态共识参与节点。
- ③ 为共识参与节点的产生设计了一套基于持有权益比例的投票机制,通过投票决定共识参与节点(记账节点)。

(6) Pool 验证池

Pool 验证池基于传统的分布式一致性技术建立,并辅之以数据验证机制,是目前区块链中广泛使用的一种共识机制。

Pool 验证池不需要依赖代币就可以工作,在成熟的分布式一致性算法基础之上,可以实现秒级共识验证,更适合有多方参与的多中心商业模式。不过,Pool 验证池也存在一些不足,如该共识机制能够实现的分布式程度不如 PoW 机制等。

4. 区块链的系统架构

区块链系统由数据层、网络层、共识层、激励层、合约层和应用层组成,如图 3-23 所示。

(1) 数据层

数据层封装了底层数据区块以及相关的数据加密和时间戳等基础数据和基本算法,主要包含区块数据、链式结构、数字签名(时间戳)、哈希函数、Merkle 树与非对称加密等。

(2) 网络层

网络层则包括分布式组网机制、数据传播机制和数据验证机制,主要有 P2P 网络结构、传



图 3-23 区块链系统架构

播机制与验证机制等。

(3) 共识层

共识层主要封装网络节点的各类共识算法,主要包含分布式一致性算法与工作量证明机制(PoW)、权益证明机制(PoS)、授权股权证明机制(DPoS)等共识机制与算法。

(4) 激励层

激励层将经济因素集成到区块链技术体系中来,主要包括经济激励的发行机制和分配机制等。

(5) 合约层

合约层主要封装各类脚本、算法和智能合约,是区块链可编程特性的基础。

(6) 应用层

应用层则封装了区块链的各种应用场景和案例。

该框架中,基于时间戳的链式区块结构、分布式节点的共识机制、基于共识算力的经济激励和灵活可编程的智能合约是区块链技术最具代表性的创新点。

3.3.3 区块链技术在金融领域的应用

区块链在国际汇兑、信用证、股权登记和证券交易所等金融领域有着潜在的巨大应用价值。将区块链技术应用在金融行业中,能够省去第三方中介环节,实现点对点的直接对接,从而在大大降低成本的同时,快速完成交易支付。主要应用包括数字货币、数字票据、跨境支付、数字资产、金融交易、融资众筹、供应链金融、互助保险、按揭业务等,如图 3-24 所示。

1. 数字货币

区块链的技术特性为数字货币发行的可能性提供了一种可选的底层技术支撑。数字货币以比特币为代表,本质上是由分布式网络系统生成的数字货币,其发行过程不依赖于特定的中心化机构。

2. 数字票据

目前票据业务主要存在三方面问题:一是票据的真实性,市场中存在假票、克隆票、刑事



票等伪造假冒票据；二是划款的即时性，即票据到期后承兑人未及时将相关款项划入持票人账户；三是违规交易，即票据交易主体或者中介机构，存在一票多卖、清单交易、过桥销规模、出租账户等违规行为。区块链数据具有不可篡改、不可伪造、带有时间戳、由共识节点共同验证和记录等特点，区块链的这些特性能够消除票据市场的中介乱象，通过智能合约编程的方式提高票据交易的效率，降低监管成本。例如，区块链可以永久地安全存储由政府机构核发的各类许可证、登记表、执照、证明、认证和记录等。

3. 跨境支付

当前跨境支付清算都需要借助第三方中介，经过开户行、中央银行、境外银行等多道程序。由于每一机构都有自己的账簿系统且互相隔离，彼此之间需要建立代理关系，并在不同系统进行记录和与交易对手进行对账及清算等，导致一笔汇款需要 2~3 天才能到账，在途资金占用量极大，而且需要支付大量的手续费。成本和效率成为跨境支付汇款的瓶颈所在。

区块链技术可以摒弃第三方中介的角色，实现点到点快速且成本低廉的跨境支付。不但可以全天候支付、实时到账、提现简便及没有隐形成本，也有助于降低跨境电商资金风险及满足跨境电商对支付清算服务的及时性、便捷性需求。

4. 数字资产

传统的资产服务如资产所有者证明、真实性公证等，均需要第三方的介入才可以完成，只有通过资产发行方、资产接收方、流通平台的三方介入，资产才可以完成整个流通过程。当前资产流通渠道有限，导致资产服务流通成本增加。此外，当资产进入流通后，需要依赖资产发行方完成使用和转移，从而限制了资产只能在发行方系统用户群内流通。

基于区块链技术能提高数字资产流通效率，降低流通成本，扩大流通范围。资产发行方均可在区块链上登记、发行任何可数字化的资产。一旦数字资产进入区块链流通，便不再依赖于资产发行方，扩大了流通范围。流通渠道由原来的中心控制变为分布式流通，降低了流通成本。区块链的交易及结算功能使得实时清算成为可能，大幅提高了数字资产流通效率。

5. 金融交易

区块链与金融市场应用有着非常高的契合度。利用区块链的不可篡改、增加信任、有效共识、智能合约、交易快速确认、可追溯等特性，可以使金融交易在去中心化系统中自发地产生信用，建立无中心机构信用背书的金融市场，实现“金融脱媒”。同时，利用区块链自动化智能合约和可编程的特点，还可以极大地降低成本和提高效率。

6. 融资众筹

区块链技术在股权登记管理、股权转让流通、智能合约等方面为融资众筹带来了深刻的变化。使用数字货币进行众筹,采用区块链协议发起和管理众筹项目,费率低、易流通、透明、稳定、可审计,智能合约还可以保证未达到预定目标时资金自动退回。

7. 供应链金融

许多人都认可供应链金融是区块链技术落地金融的最佳场景。区块链在供应链金融中的应用包括供应链应收账款融资、供应链授信融资、区块链合同存证、预付卡系统、资金数字化、积分联盟系统、商品生命周期跟踪等。

小资料 3-5

供应链金融

供应链金融(Supply Chain Finance, SCF)是商业银行信贷业务的一个专业领域(银行层面),也是企业尤其是中小企业的一种融资渠道(企业层面)。指银行向客户(核心企业)提供融资和其他结算、理财服务,同时向这些客户的供应商提供贷款及时收款的便利,或者向其分销商提供预付款代付及存货融资服务。简单地说,就是银行将核心企业和上下游企业联系在一起提供灵活运用的金融产品和服务的一种融资模式。

与传统的保理业务及货押业务(动产及货权抵/质押授信)不同,保理和货押只是简单的贸易融资产品,而供应链金融是核心企业与银行间达成的,一种面向供应链所有成员企业的系统性融资安排。

一般来说,一个特定商品的供应链从原材料采购,到制成中间及最终产品,最后由销售网络把产品送到消费者手中,将供应商、制造商、分销商、零售商、直到最终用户连成一个整体。在这个供应链中,竞争力较强、规模较大的核心企业因其强势地位,往往在交货、价格、账期等贸易条件方面对上下游配套企业要求苛刻,从而给这些企业造成了巨大的压力。而上下游配套企业恰恰大多是中小企业,难以从银行融资,结果最后造成资金链十分紧张,整个供应链出现失衡。“供应链金融”最大的特点就是在供应链中寻找出一个大的核心企业,以核心企业为出发点,为供应链提供金融支持。一方面,将资金有效注入处于相对弱势的上下游配套中小企业,解决中小企业融资难和供应链失衡的问题;另一方面,将银行信用融入上下游企业的购销行为,增强其商业信用,促进中小企业与核心企业建立长期战略协同关系,提升供应链的竞争能力。

(资料来源:百度百科)

8. 互助保险

区块链能够实现对新兴保险业务模式的革新,增强保险市场对风险的记录能力、透明度、识别准确度和反应速度。区块链技术可以实现真正的P2P或众筹保险模式,基于智能合约建立按需定制的保险合约,替代传统的保单协议,使管理过程更简单、更自动化、更透明、成本更低并使合约执行速度更快。同时保险公司的角色也将逐渐变为专业咨询和互惠池机制管理,而不是直接承担风险。

9. 按揭业务

区块链技术用于按揭业务。在按揭申请流程中,牵涉递表及审批等,文件繁复。但在区块链“去中心化”下,参与这项业务的各方人士获得所需文件之余,亦能确保文件真实,而过往记

录几乎不能篡改,亦可以追溯,大大提升伪造文件难度。在按揭业务中引入区块链技术,除了审批速度加快以外,客户感受并不会很明显,因为区块链属于后台技术,但随着加入的机构越来越多,未来的发展和创新空间越来越大。

3.4 人工智能技术

3.4.1 人工智能概述

1. 人工智能的概念

在 20 世纪 50 年代以来的三次技术革新浪潮中,学界和业界对人工智能的理解众说纷纭,科技和商业的多元化导致人们对人工智能的定义、发展以及表现形式的理解各异。计算机科学理论奠基人图灵(Alan Mathison Turing)在论文《计算机器和智能》中提出了著名的“图灵测试”——如果一台机器能够与人展开对话(通过电传设备),并且会被误以为也是人,那么这台机器就具有智能。人工智能之父马文·明斯基(Marvin Minsky)则将其定义为“让机器做本需要人的智能才能够做到的事情的一门科学”,这也比较接近当前人们对人工智能的理解。而代表人工智能的另一条路线——符号派的赫伯特·西蒙(Herbert A. Simon)认为,智能是对符号的操作,最原始的符号对应于物理客体。

全面认识人工智能之所以困难,是有客观原因的。人工智能是一个非常广泛的领域。当前人工智能涵盖很多学科,具体可以归纳为 6 个学科:①计算机视觉(暂且把模式识别、图像处理等问题归入其中);②自然语言理解与交流(包括对话,暂且把语音识别、合成归入其中);③认知与推理(包含各种物理和社会常识);④机器人学(机械、控制、设计、运动规划、任务规划等);⑤博弈与伦理(多代理人的交互、对抗与合作,机器人与社会融合等);⑥机器学习(各种统计的建模、分析工具和计算的方法)。上述这些学科目前正处于交叉发展、走向统一的过程中。

从单独的领域很难为人工智能赋予一个比较全面的定义,下面从技术目标的角度对人工智能进行定义。

人工智能(Artificial Intelligence, AI),是一门研究、开发用于模拟、延伸和扩展人的智能的理论、方法、技术及应用系统的新技术科学,它的目标就是用机器去实现所有目前必须借助人类智慧才能实现的任务。

人工智能是计算机科学的一个分支,它试图了解智能的实质,并生产出一种新的能以与人类智能相似的方式做出反应的智能机器。该领域的研究包括机器人、语言识别、图像识别、自然语言处理和专家系统等。人工智能发展到今天,理论和技术日益成熟,应用领域也不断扩大,可以设想未来人工智能带来的科技产品将会是人类智慧的“容器”。人工智能是对人的意识、思维的信息过程的模拟,它虽然不是人的智能,但能像人那样思考,也可能超过人的智能。

经过半个多世纪的发展,人工智能已经度过了简单模拟人类智能的阶段,发展成为一门研究人类智能活动规律,构建具有一定智能的人工系统及硬件,以使其能够进行需要人的智力才能进行的工作,并能够对人类智能进行拓展的学科。

2. 人工智能的分支

人工智能是一门涉及众多领域的综合学科,从应用的技术上看,人工智能技术主要有四个分支。

(1) 模式识别

模式识别是指对表征事物或者现象的各种形式的信息(数值、文字、逻辑关系等)进行处理

和分析,以及对事物或者现象进行描述、分析、分类、解释的过程,如信用卡号的辨识。在模式识别的过程中,以图像分析和处理技术为主的一类技术是它的核心。

(2) 机器学习

机器学习是研究计算机如何去模拟或者实现人类学习行为的一门学科,它通过对人类学习行为的模拟,获取新的知识或者技能,重新组织已有的知识结构,实现不断完善自身性能的目标,达到操作者的特定要求。

(3) 数据挖掘

数据挖掘的兴起得益于大数据和云计算技术的发展,全新的数据结构和数据处理方式使得数据价值的实现有了新的目标。数据挖掘就是依靠算法在海量的数据中搜索和挖掘有用的信息,它应用于市场分析、科学探索、疾病预测、金融征信等各个领域。

(4) 智能算法

智能算法是人工智能的核心,前三个分支都是人工智能技术的应用领域,而智能算法是这三个分支的重要基础,其研究对象就是计算机在处理和解决问题时的特定模式算法,可以将其理解为计算机的思维方式。

3. 人工智能的发展

回顾人工智能的发展历程,可以从时间和技术两个层次来展开。

1) 时间上

(1) 萌芽期

1943年,人工神经网络和数学模型建立,人工神经网络研究时代开启;1950年,计算机与人工智能之父图灵发表论文《机器能思考吗?》,提出“图灵测试”,这是人类科学史上对人工智能的早期思考。

(2) 启动期

1956年,达特茅斯会议召开,会议上正式提出了人工智能的说法,标志着人工智能的诞生,也使这一年成为人工智能元年。这一时期,人工智能研究在国际学术界的兴起,罗素《数学原理》算法被全部证明,学术交流日益频繁,算法不断发展也带动了人工智能的进步。

(3) 消沉期

1969年,由于时代的限制,科学技术的发展跟不上理论的进步,作为主要流派的连接主义与符合主义进入消沉期,四大预言并无进展,在计算能力的限制下,国家及公众对人工智能的信心持续减弱。

(4) 突破期

1986年,反向传播(Back Propagation, BP)算法开始研究,第五代计算机开始研制,专家系统的研究和应用艰难前行。随着半导体技术的发展,计算能力逐步提高,人工智能的发展开始有所突破。

(5) 发展期

BP算法实现,人工神经网络被广泛认知,基于人工神经网络的算法研究突飞猛进,计算机硬件能力快速提升。随着分布式网络的构建,人工智能的计算成本得以降低。

(6) 高速发展期

2006年,深度学习被提出,人工智能再次得到突破性的发展;2010年,移动互联网发展,人工智能应用场景开始增多;2012年,深度学习算法在语音识别和视觉识别上实现突破,同时融资规模开始快速增长,人工智能商业化高速发展;2016年,在以往被认为是机器

“无法取胜”的围棋比赛中, AlphaGo 成功击败人类围棋世界冠军, 这被认为是人工智能的重大突破。

2) 技术上

从技术发展的角度来看, 人工智能一直在曲折中发展。1956 年达特茅斯会议上一群科学家通过集中讨论, 引出了人工智能这个概念。之后, 人工智能经历了短时间的萌芽期, 人工智能的各种思路和设想被纷纷提出, 使人们对人工智能美好的前景有着极高的期待。但是, 随着时间的推移, 在技术一直无法取得突破的情况下, 人工智能领域曾看不到前进的方向。

1977 年在第五届国际人工智能会议上, 美国斯坦福大学计算机科学家费根鲍姆正式提出了知识工程的概念, 随后各类专家系统得以发展, 大量商品化的专家系统被推出。但好景不长, 因为这些专家系统的学习能力非常有限, 满足不了科技和生产提出的新要求, 人工智能离人们的期待还有着很大的距离。在随后的 20 多年中, 人工智能的发展几乎处于停滞不前的状态。

进入 21 世纪, 科学技术在三个领域的发展使得人工智能这个曾被认为是空中楼阁的概念有了实现的可能, 这三个领域是数据收集与整理、算法以及高性能计算技术。它们的代表就是大数据、机器学习和云计算。大数据解决了数据的来源问题; 机器学习尤其是深度学习为人工智能的发展突破了算法的瓶颈, 而以云计算为代表的分布式计算技术为这一切的实现提供了硬件上的可能。这使得人工智能技术走下神坛, 成为现实。可以说, 正是大数据、机器学习以及云计算的结合, 才使人工智能获得真正意义上的诞生。

3.4.2 人工智能的核心技术

人工智能的核心技术主要包括计算、数据、算法三个方面的技术, 如图 3-25 所示, 具体体现在以云计算为代表的计算技术、以大数据为代表的海量数据采集和处理技术, 以及以深度学习算法为代表的机器学习算法。

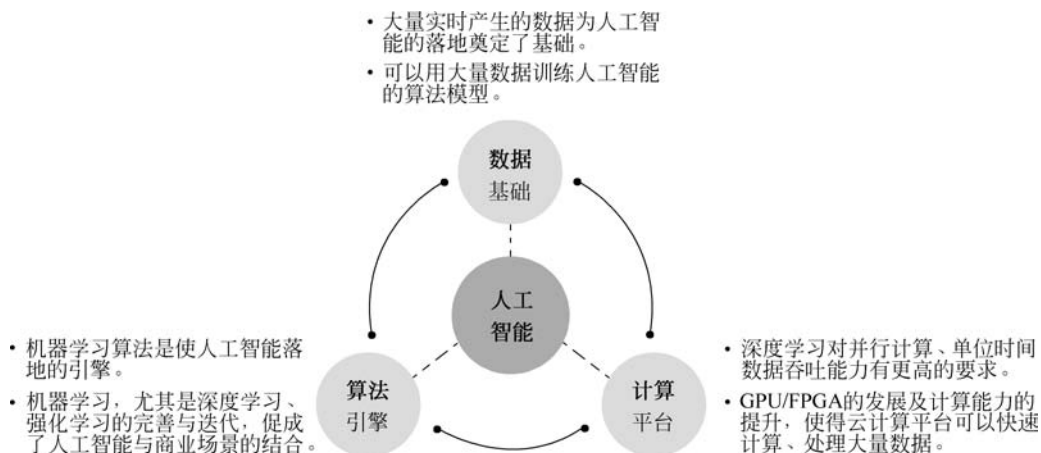


图 3-25 人工智能的核心技术

首先, 人工智能对计算能力的要求很高, 而以前研究人工智能的科学家往往受限于单机的计算能力, 而需要对数据样本进行裁剪, 以使得能够在单机中对数据进行建模和分析, 导致模型的准确率降低。随着云计算技术和芯片处理能力的迅速发展, 人们可以利用成千上万台机

器进行并行计算,尤其是图形处理器(GPU)、FPGA 以及人工智能专用芯片(如 Google 的张量处理器 TPU)的发展为人工智能的落地提供了基础计算平台,使得人工智能的应用成为现实。

其次,随着互联网的飞速发展,在线数据变得非常丰富,多源、实时、大量、多类型数据可以从不同的角度对现实进行更为逼真的描述,而利用以大数据为代表的数据采集和处理技术可以挖掘数据之间多层次的关联关系,为人工智能的应用奠定数据源基础。

最后,算法的发展,尤其是神经网络之父 Geoffrey Hinton 于 2006 年发表的论文,开启了深度学习在学术界和工业界的研究和应用浪潮,基于人工神经网络的深度学习算法成为人工智能应用落地的核心引擎。

上述三个核心技术相辅相成,相互依赖,相互促进,使得人工智能有机会从专用的技术发展为通用的技术,融入到各行各业之中。

3.4.3 人工智能的应用领域

目前,人工智能的主要的应用领域包括计算机视觉、自然语言处理、智能机器人等。

1. 计算机视觉

计算机视觉主要是指利用当今快速发展的计算机技术对人类的视觉系统进行模拟,以能够确定物体的位置和运动状态,并能够识别物体,达到代替人类眼睛的目的。一般情况下,计算机视觉领域在应用人工智能技术时需要经过三个步骤:检测目标、识别目标、识别行为。现阶段,人工智能在计算机视觉领域中的典型应用是人脸识别系统、瞳孔识别系统和指纹识别系统。此外,人工智能在计算机视觉领域的物体场景识别方面尚没有成熟的技术和系统,这主要是由于物体具有复杂性和多样性的特点,虽然可以利用人工智能技术对物体的外貌和特征进行识别,但准确性不高,因而仍然需要对人工智能视觉技术展开更加深入的研究。

2. 自然语言处理

自然语言处理是人工智能的重要应用领域,其主要的研究内容为人机通过自然语言实现有效的互动,而其主要使用的技术为自然语言信息处理技术。人工智能在自然语言处理领域中的典型应用有客服服务、机器人聊天、机器同声传译等。在自然语言信息处理技术中,自然语言识别技术已经相当成熟,自然语言准确识别率基本上达到 95% 以上,百度、科大讯飞(<https://www.iflytek.com>)等公司对该技术均进行了积极且有效的应用。

3. 智能机器人

智能机器人主要是指由人类进行操控,但其自身具有比较发达的“大脑”,能够独立进行自我控制的机器人。智能机器人主要包括:感觉要素,用于对外部环境进行识别;运动要素,用于与外部环境产生有效的互动;思考要素,用于对所接收到的外部信息进行处理,进而给出准确的回应。现阶段,服务机器人、工业机器人等智能机器人都已经得到了一定的应用,而且将来会有更加广阔的应用市场和发展空间,这是因为它能够给人类的生活带来较大的便利性。

除互联网企业外,一些传统金融机构、金融科技公司在人工智能领域也加大了投入,并在人工智能的垂直细分领域得到了快速发展。其开发的产品已应用于证券行业的智能投顾、量化交易、风险管理、信用评估、远程开户、票据影像识别等金融细分领域。

目前,人工智能就研究、解释和模拟人类智能、智能行为及其规律这一总目标来说,已经迈出了可喜的一步,某些领域已取得了很大的进展。但是从整个发展过程来看,人工智能仍面临着不少难题。人工智能在发展过程中所面临的难题主要有以下三个:一是计算机博弈的困难,尤其是对于博弈问题状态空间庞大,且存在多人对弈、随机性博弈的问题,目前计算机难以模拟实现;二是理论的不成熟,人工智能控制理论的发展存在不同的理论和算法只适用于特定领域或工程背景的问题,理论的通用性和可移植性较弱,到目前为止,人工智能理论的发展尚未形成一个完整而系统的理论结构框架;三是模式识别的困惑,目前人工智能理论和技术的发展远远达不到模拟人的识别手段和形象思维能力的程度,也难以处理非结构化的问题。

3.5 移动互联网技术

金融电子商务的兴起得益于互联网技术,金融电子商务的普及则得益于移动通信技术,得益于智能手机的普及,得益于移动互联网技术。

3.5.1 移动互联网概述

1. 移动互联网定义

移动互联网是将移动通信和互联网二者结合起来,成为一体。它是互联网的技术、平台、商业模式和应用与移动通信技术相结合的产物。

移动互联网第一次把互联网放到人们的手中,实现 24 小时随身在线的生活。信息社会给人类最大的承诺就是随时随地随身查找信息、处理工作、保持沟通、进行娱乐,这个承诺已经从梦想变成现实。就像中国移动的广告语所说——“移动改变生活”,移动互联网给人们的生活方式带来翻天覆地变化。移动互联网成为当前推动产业和经济发展最强有力的技术力量。

2. 移动互联网的发展历程

讨论移动互联网的发展都是从 2000 年左右开始,可以划分为不同阶段,当然不同的人有不同的分法。但无论是 3 个阶段或者是 5 个阶段,都总体能够反映移动互联网发展的几个重要时段。

(1) 萌芽期(2000—2003 年)

2001 年 11 月,中国移动的“移动梦网”正式开通。当时官方的宣传称,手机用户可通过“移动梦网”享受到移动游戏、信息点播、掌上理财、旅行服务、移动办公等服务。

(2) 发展期(2003—2007 年)

自 2004 年移动互联门户开启后,先后出现了搜索、音乐、阅读、手游等领域的多种无线企业,在这个发展期,所有的企业其实都很迷茫,谁都不清楚未来是什么样子。而商业模式之争就成了当时热议的话题。

(3) 提速期(2007—2010 年)

在 2007 年,iPhone 和 Android 系列设备占领移动终端市场。有人说:“得终端者得天下。”所以不同厂商纷纷在移动互联网终端领域展开激烈竞争,以求掌握移动互联网的入口。

(4) 黄金增长期(2010—2013 年)

2009 年 1 月,工信部举办牌照发放仪式,确认国内 3G 牌照发放给三家运营商。在黄金增长期,涌现出一大批社交、阅读等领域的产品软件,如 iPad、新浪微博、微信等。而在 2011—2012 年,宽带中国战略全面启动,这使得宽带首次成为国家战略性公共基础设施。

(5) 全面发展期(2013 年至今)

在移动互联网全面发展的这一时期,又经历了三个阶段。

- ① 提供便捷生活服务场景,培养用户习惯。
- ② 通过内容布局提升用户黏性,注重变现和创新商业模式。
- ③ 多入口模式发展,超级巨头多元布局,各领域开始洗牌。

这短短的几年时间,移动支付、网约车、众筹、外卖、社交电商、新零售、共享单车、移动直播、短视频、小程序等出现在人们的视野中,让大家的生活质量得到了很大提升。

3. 移动互联网基本特点

与传统的 PC 互联网相比较,移动互联网具有五个鲜明的特性。

(1) 便捷性和便携性

移动互联网实际是一个立体的网络,GPRS、3G、4G 和无线局域网 WLAN 或 WiFi 构成的无缝覆盖,使得移动终端具有通过上述任何形式方便联通网络的特性;移动互联网的基本载体是移动终端。顾名思义,这些移动终端不仅仅是智能手机、平板电脑,还有可能是智能眼镜、手表、服装、饰品等各类随身物品。它们属于人体穿戴的一部分,随时随地都可使用。

(2) 即时性和精确性

由于有了上述便捷性和便利性,人们可以充分利用生活中、工作中的碎片化时间,接受和处理互联网的各类信息。不再担心有任何重要信息、时效信息被错过了。无论是什么样的移动终端,其个性化程度都相当高。尤其是智能手机,每一个电话号码都精确地指向了一个明确的个体,因此移动互联网能够针对不同的个体,提供更为精准的个性化服务。

(3) 感触性和定向性

这一点不仅仅是体现在移动终端屏幕的感触层面,更重要的是体现在照相、摄像、二维码扫描,以及重力感应、磁场感应、移动感应,温度、湿度感应等无所不及的感触功能。而采用基于位置的服务(Location Based Services,LBS)不仅能够定位移动终端所在的位置,甚至可以根据移动终端的趋向性,确定下一步可能去往的位置,使得相关服务具有可靠的定位性和定向性。

(4) 业务与终端、网络的强关联性和业务使用的私密性

由于移动互联网业务受到了网络及终端能力的限制,因此,其业务内容和形式也需要适合特定的网络技术规格和终端类型。在使用移动互联网业务时,所使用的内容和服务更私密,如手机支付业务。

(5) 网络的局限性

移动互联网业务在便携的同时,也受到了来自网络能力和终端能力的限制。在网络能力方面,受到无线网络传输环境、技术能力等因素限制;在终端能力方面,受到终端大小、处理能力、电池容量等的限制。

4. 移动互联网和 PC 互联网的区别

移动互联网已经完全渗入到人们生活、工作、娱乐的方方面面了。以上这 5 大特性,构成

了移动互联网与 PC 互联网完全不同的用户体验生态。移动互联网和 PC 互联网最大的区别是终端不同。移动互联网的终端是手机,随时随地移动,而 PC 互联网的终端是台式机,移动性较差。本质上讲,“小巧轻便”及“通讯便捷”的特点,决定了移动互联网与 PC 互联网的根本不同。虽然它们各自的发展趋势不同,但相互之间仍有许多关联之处。移动终端的发展,将会大幅替代目前作为上网终端主流的 PC,所以针对移动终端的特点(便携、屏幕尺寸、输入方式、拍照、定位等功能)会衍生出各类更先进的应用或解决方案。另一个需要注意的是,PC 作为主要的上网终端,真正的优势在于内容制作,而不是内容获取,所以 PC 未来会越来越变成少数人的工具,而不是现在的标配。

5. 移动互联网的应用领域

移动互联网的浪潮正席卷到社会的方方面面,新闻阅读、视频节目、电商购物、公交出行等热门应用都出现在移动终端上,在苹果和安卓应用商店的下载量已达到数百亿次,而移动用户规模更是超过了 PC 用户规模。这让企业级用户意识到移动应用的必要性,纷纷开始规划和摸索进入移动互联网,客观上加快了企业级移动应用市场的发展。当然在应用不断推广的过程中,也崛起了一批移动互联网公司。

移动互联网的应用主要有以下领域。

(1) 衣食住行

这些公司利用了吃喝玩乐本地化的特征,运用无线互联网给用户带来全新的感受。

(2) 健康和医疗行业

通过移动互联网感应设备,能够及时地反映健康和运动当中的一些数据,对用户来说就是巨大的体验改变。

(3) 通信

中国最重要的无线互联网应用是微信的崛起,这是巨大的创新。当然还有其他的各种即时通信软件。

(4) 搜索

这是非常传统的互联网应用,但已在手机上面有绝佳的展现。结合手机跟地理位置以及语言相关的搜索,在未来搜索市场里更有巨大的成长空间。

(5) 金融服务

比如支付宝、微信等支付,相互之间的竞争非常激烈。

(6) 游戏娱乐行业

手机游戏用户群是网游和网页游戏的综合,这是真正全面大众的游戏方式,而且可以把很多碎片时间利用起来。中国网游领域已经产生了多个大型企业。

(7) 广告传媒

手机上的广告传媒展现了跟传统互联网不同的形式,由于其精确性,在数据挖掘上有更强的开发能力。

(8) 垂直社交

垂直社交是对一群兴趣相投的人的交流方式的称呼。垂直社交与一般网络社交相比,会有针对性地投放广告和信息,能满足用户对某个方面的特别需求,也就是说垂直社交具有商业价值。在垂直社交领域,手机扮演了非常重要的角色。根据最新研究报告,垂直赛道未来依然存在“逆袭”的机会,产品创新、技术迭代均能获得新的增长水平。

(9) 企业服务

移动互联网为企业服务带来了新的机会,非常重要的一个应用就是企业的社交,一个企业在商务环境当中也需要建立一个社交的网络,通过移动互联网、云端的应用可能会给企业带来更好的效果。

综合以上应用,可以总结出移动互联网应用的特点如下。

(1) 手机成为娱乐终端

随着移动应用程序的普及,手机已经不再只是一个基本通讯和信息传递的终端,而是一个人们随身携带的娱乐终端。这一变化,催生了巨大的手机游戏娱乐产业。

(2) 手机真正解决商业需求

可以说从 2011 年起,消费群体就逐步走入了移动生活。使用智能手机与平板电脑的用户群正以惊人的速度增长,用户的消费方式,消费习惯和消费行为都在随着移动互联网的发展而改变。

(3) 移动搜索的广泛运用

移动搜索也已经成为人们生活中最重要的一种消费,最直接的表现就是几乎每个智能手机上都装有电子地图,已经成为人们衣食住行的标准配置。

(4) 本地化趋势越来越强

移动互联网服务使人们可以“实时实地”获取各种信息,这也正是移动互联网的魅力所在。移动互联网在提供各种基础性的服务时,必须首先满足本地化服务需求。

6. 移动互联网发展趋势

(1) 移动互联网超越 PC 互联网,引领发展潮流

移动互联网流量将占互联网流量主导。有线互联网是互联网的早期形态,移动互联网(无线互联网)是互联网的未来。PC 机只是互联网的终端之一,移动装置的普及是支撑移动互联网发展的关键,智能手机、平板电脑、电子阅读器已经成为重要终端。电视机、车载设备、冰箱、微波炉、抽油烟机、照相机,甚至眼镜、手表等穿戴设备,都正在变成终端。

(2) 移动互联网和传统行业融合,催生新的应用模式

在移动互联网、云计算、物联网、人工智能等新技术的推动下,传统行业与互联网的融合正在呈现出新的特点,平台和模式都发生了改变。一方面可以作为业务推广的新手段,如食品、餐饮、娱乐、航空、汽车、金融、家电等传统行业的 App 和企业推广平台;另一方面也重构了移动端的业务模式,如医疗、教育、旅游、交通、传媒等领域的业务模式的改造。今天,在手机上完成飞机的座位选号、医院的看病挂号等都已经是非常普通的事了。

(3) 移动互联网商业模式多样化

成功的业务需要成功的商业模式来支持。移动互联网业务的新特点为商业模式创新提供了空间。随着移动互联网发展应用的普及,网络、终端、用户等方面已经具备了坚实的基础,很多领域应用已经渡过了前期的培育期,不盈利的情况开始改变,移动互联网已融入主流生活与商业社会,移动游戏、移动广告、移动电子商务、移动视频等业务模式流量变现能力快速提升。移动互联网消费每年都在持续增长,固定互联网消费呈下降趋势。

(4) 用户体验的不断改进

智能手机屏幕从不同大小屏幕的移动终端角度来看,其用户体验是不一样的,适应小屏幕的智能手机的网页应该轻便化、轻质化,它承载的广告也必须适应这一要求。目前大量互联网业务迁移到手机上,为适应平板电脑、智能手机及不同操作系统,开发出了不同的 App。技术

上看,HTML 5 的自适应能力较好地解决了不同大小、不同规格的屏幕阅读体验问题,但是还远未达到轻便化、轻质化、人性化的要求,仍缺乏良好的用户体验。另外,目前 iOS、Android 两大系统各自独立,相对封闭、割裂,这种隔绝不符合互联网互通互联的精神。不同品牌、类型的移动终端都应该能互联互通,这是用户的期待,也是发展趋势。

(5) 大数据挖掘成为蓝海,人工智能技术与产业结合推动爆发式增长

随着移动宽带技术的迅速提升,更多的传感设备、移动终端随时随地地接入网络,加之人工智能、云计算、物联网等技术的带动,中国移动互联网步入“大数据”时代。当前 BAT 等巨头调整组织架构,提升 to B 业务的战略地位,各家突破方向虽有不同,但投资布局都聚焦在产业互联网的技术基础层面,包括 AI、云计算、大数据、物联网等。目前的移动互联网领域,仍然是以精准营销为主,但未来随着大数据相关技术的发展,人们对数据挖掘的不断深入,针对用户个性化定制的应用服务和营销方式将成为发展趋势,它将是移动互联网的另一片蓝海。人工智能通过搭载移动终端,构建智慧生态,而以“移动互联网+人工智能+物流共享”为标志的智慧物流平台必能成为物流行业新趋势。

(6) 5G 商业化给行业带来冲击

5G 时代智能终端和物联网将最先受益,产业链上下游创新企业将迎来脱颖而出和弯道超车的机会。5G 将率先应用在视频内容消费、产业互联网、远程诊断、物联网、车联网等方面来变革用户的使用场景。

在移动互联网时代,传统的信息产业运作模式正在被打破,新的运作模式正在形成。对于手机厂商、互联网公司、消费电子公司和网络运营商来说,这既是机遇,当然也是挑战。而他们积极参与到移动互联网的市场竞争中,最终受益的是所有的使用者。

3.5.2 移动互联网技术架构

移动互联网的出现迎来了移动网和互联网融合发展的新时代,移动网和互联网的融合也会是在应用、网络和终端多层面的融合。为了能满足移动互联网的特点和业务模式需求,在移动互联网技术架构中要具有接入控制、内容适配、业务管控、资源调度、终端适配等功能。构建这样的架构需要从终端技术、承载网络技术、业务网络技术各方面综合考量。

1. 移动互联网的体系

如图 3-26 所示为移动互联网的典型体系架构模型。

1) 业务应用模块

提供给移动终端的互联网应用。这些应用中包括典型的互联网应用,比如网页浏览、在线视频、内容共享与下载、电子邮件等;也包括基于移动网络特有的应用,如定位服务、移动业务搜索以及移动通信业务(短信、彩信、铃音等)。

2) 移动终端模块

从上至下包括终端软件架构和终端硬件架构。

(1) 终端软件架构

包括应用 App、用户 UI、支持底层硬件的驱动、存储和多线程内核等。

(2) 终端硬件架构

包括终端中实现各种功能的部件。

3) 网络与业务模块

从上至下包括业务应用平台和公用接入网络。

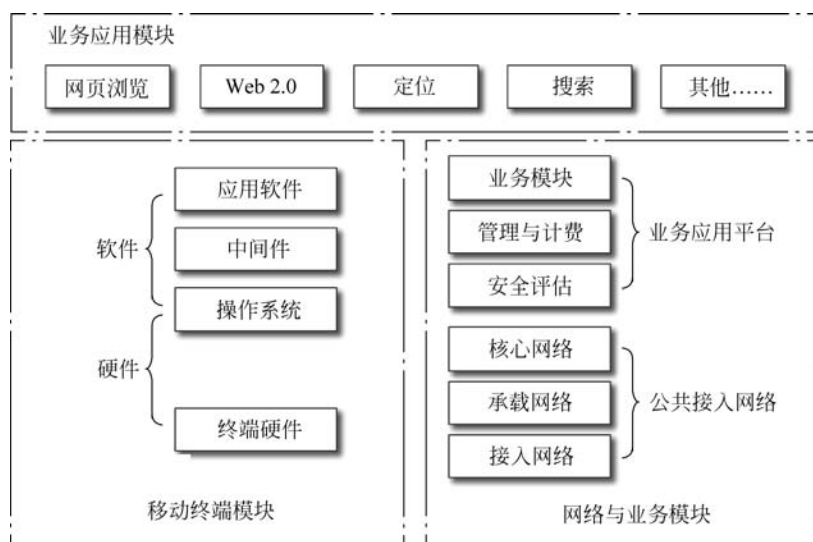


图 3-26 移动互联网的体系架构

(1) 业务应用平台

包括业务模块、管理与计费系统、安全评估系统等。

(2) 公共接入网络

包括核心网络、承载网络和接入网络等。

2. 移动互联网的业务模型

从移动互联网中端到端的应用角度出发,移动互联网的业务模型可分为五层。

(1) 第一层 移动终端

支持实现用户 UI、接入互联网、实现业务互操作。终端具有智能化和较强的处理能力,可以在应用平台和终端上进行更多的业务逻辑处理,尽量减少空中接口的数据信息传递压力。

(2) 第二层 移动网络

包括各种将移动终端接入无线核心网的设施,比如无线路由器、交换机、BSC、MSC 等。

(3) 第三层 网络接入

网络接入网关提供移动网络中的业务执行环境,识别上下行的业务信息、服务质量要求等,并可基于这些信息提供按业务、内容区分的资源控制和计费策略。网络接入网关根据业务的签约信息,动态进行网络资源调度,最大程度地满足业务的 QoS(Quality of Service)要求。

(4) 第四层 业务接入

业务接入网关向第三方应用开放移动网络能力 API 和业务生成环境,使互联网应用可以方便地调用移动网络开放的能力,提供具有移动网络特点的应用。同时,实现对业务接入移动网络的认证,实现对互联网内容的整合和适配,使内容更适合移动终端对其的识别和展示。

(5) 第五层 移动网络应用

提供各类移动通信、互联网以及移动互联网特有的服务。

另外,技术团队要始终把安全放在第一位,竭尽全力保障投资人的资金安全与信息安全。参照国家信息系统安全等级保护的要求,制定综合的安全治理措施,主要包括 3 个方面。

一是基础技术设施安全建设。采用企业级防火墙、HTTPS 数据传输加密、分布式数据存储与备份、抗分布式拒绝服务(Distributed Denial of Service,DDOS)攻击,跟踪最新漏洞,及时进行系统升级。

二是提高代码的安全性。制定代码规范和各种开发规范,确保开发人员能够写出安全的代码;开发代码扫描工具,扫描代码;代码审查,代码交叉审核;单元测试与自动化测试。

三是建立监控与反馈系统。及时发现潜在的问题,化被动为主动;为可能发现的问题,制定应急预案;监控重点敏感数据与功能,发现异常及时进行阻断和报警。

最后,技术团队要为整个技术平台,制定出长期的改善目标。比如应该包括:持续改善系统架构,更好地支持业务扩展;降低系统耦合,提升对变化的响应速度;建立更完整的公共平台、基础框架、基础类库,提高开发效率;合理地增加或减少系统间交互,提升系统性能稳定性;完善配置、监控、预警、日志系统,提升系统运维效率及发现问题的速度。

3. 移动互联网的关键技术

移动互联网的关键技术包括无线应用协议、移动 IP 技术、移动操作系统、移动标志语言等。这里仅对无线应用协议及移动 IP 技术做简单的介绍。

1) 无线应用协议(WAP)

无线应用协议(Wireless Application Protocol,WAP)是一项开放性、全球性的网络通信协议,它使移动互联网有了一个通行的标准,其目标是将互联网的信息及业务引入移动终端之中。

(1) WAP 的产生和发展

无线应用协议(WAP)的提出和发展是基于在移动中接入互联网的需求。1997 年 6 月,Phone.com 与 Nokia、Ericsson、Motorola 合作建立了 WAP 论坛,目的就是为在移动通信中使用互联网业务制定统一的应用标准。WAP 论坛成立后,受到业界的广泛关注,目前已有 200 多个公司加入成为论坛成员,包括全球最主要的电信运营公司、电信设备制造商和软件供应商。WAP 论坛的成员代表了全球 95%手机市场,数亿的手机用户。正是由于 WAP 论坛成员具有广泛的代表性,其制定的 WAP 规范具有大多数厂商设备可以互操作的特点,所以 WAP 有望成为业界广泛接受和使用的无线信息网络连接方式。

(2) WAP 的体系结构

WAP 系统包括 WAP 网关、WAP 内容服务器和 WAP 移动终端,如图 3-27 所示。



图 3-27 WAP 的体系结构

其中 WAP 网关起着协议的翻译和转换作用,是联系无线通信网络与互联网的桥梁。网关与服务器之间是基于互联网的通信,即通过 HTTP 协议进行通信,这就意味着服务的提供者几乎可以不改变信息的内容,只要增加网点设备就可以向移动用户提供信息服务;WAP 内容服务器存储着大量的信息,供 WAP 手机用户访问、查询、浏览。

典型的 WAP 应用系统定义了三类实体:具有 WAP 用户代理功能的移动终端、WAP 网

关/代理、源数据服务器。

(3) WTA 无线电话应用

除了无线应用环境和协议外,WAP 标准还定义了无线电话应用,它使得 WAP 可以很好地与目前电信网络中现存的各种先进电信业务相结合。图 3-28 描述了两种典型的 WAP 应用组网连接方式。

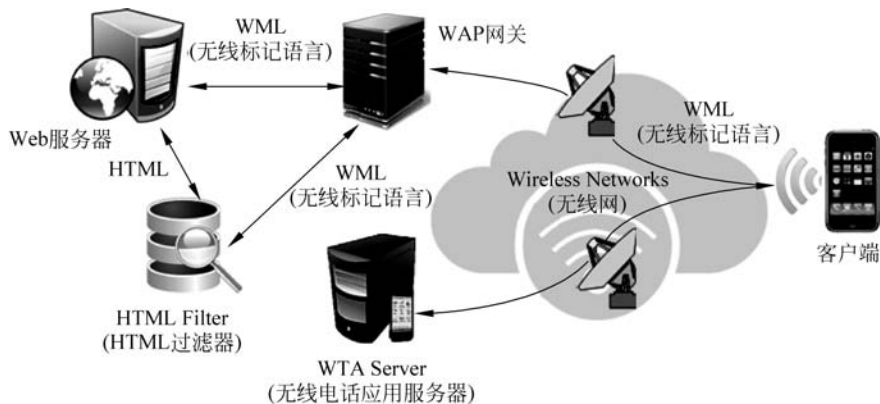


图 3-28 典型的 WAP 应用组网连接方式

(4) WAP 的应用

常见的 WAP 应用是使用具有 WAP 功能的移动终端直接连接互联网收发电子邮件,浏览交通状况、气象信息、娱乐资讯,或者与智能网结合访问计费、修改个人数据等。

WAP 最有潜力的应用是与金融结合,实现移动中的金融服务。例如,随时参与证券交易,使用移动网络银行业务,在移动中实现网上支付。以前你可能随身携带钱包、电话本、信用卡、手机等,而现在你只需携带一部具有 WAP 功能的移动电话,就可以满足打电话、付账、买车票、管理个人工作安排等各种需求。

2) 移动 IP 技术

移动 IP 技术通过在网络层改变 IP 协议,从而实现移动计算机在互联网中的无缝漫游。移动 IP 技术使得节点在从一条链路切换到另一条链路上时,无须改变它的 IP 地址,也不必中断正在进行的通信。移动 IP 技术在一定程度上能够很好地支持移动电子商务的应用。

无线接入中的移动 IP 技术使得人们一直梦想的无处不在的多媒体全球网络连接成为可能,它适应了普遍计算时代的一切需求。可以肯定,基于移动 IP 技术的第五代移动通信系统和互联网网络相结合,提供高速、高质量的多媒体通信业务必将是大势所趋。

移动 IP 技术为移动节点提供了一个高质量的实现技术,可应用于用户需要经常移动的所有领域。如通过无线网络,用户的笔记本电脑可以随时随地地上网,通过 IP 技术还可以与公司的专用网相连;扩展移动 IP 技术,还可以使一个网络移动,即把移动节点改成移动网络。它的实现可以简单地认为把原先的移动节点所做的工作改成移动网络中的路由器所做的工作,这种技术还会广泛地应用于轮船、列车等活动网络中。

移动 IP 不是移动通信技术和互联网技术的简单叠加,也不是无线语音和无线数据的简单叠加,它是移动通信和 IP 的深度融合,也是对现有移动通信方式的深刻变革。为适应快速增长的数据型业务需求,人们需要的是一个以包交换为基础的无线网络,这种新型网络结构正是移动 IP 未来的结构。移动 IP 将是移动技术和 IP 技术的深度融合,它将真正实现语音和数据

的业务融合,移动 IP 的目标是将无线语音和无线数据综合到一个技术平台上传输,这一平台就是 IP 协议。移动通信的 IP 化进程将分为三个阶段:首先是移动业务的 IP 化;然后是移动网络的分组化演进;最后是在第三代移动通信系统中实现全 IP 化。

3.5.3 移动互联网在金融领域的应用

移动互联网金融是指使用移动智能终端及移动互联技术处理金融企业内部管理及对外产品服务的解决方案。在这里,移动终端泛指以智能手机为代表的各类移动设备,其中智能手机、笔记本电脑或平板电脑、无线 POS 机目前应用范围较广。

1. 移动银行

简单地说,就是以手机、掌上电脑(Personal Digital Assistant,PDA)等移动终端作为银行业务平台中的客户端来完成某些银行业务。移动银行应用包括服务于内部员工的企业应用以及服务于外部客户的产品应用。

(1) 内部企业应用

常见的移动办公就属于典型的企业应用,该类应用的核心价值在于提高企业内部的工作效率、降低企业运营成本,提供更方便的业务流程帮助企业员工带来更高的效益。目前常见的银行内部企业应用类型包含移动营销、移动办公、移动客户关系管理、移动数据报表、移动信贷。

(2) 外部产品应用

移动银行是银行提供的最常见的对外服务移动产品,该类应用的核心价值在于增加银行的服务渠道,在提供更方便的服务同时,不但大大降低了传统渠道的成本,还可以带来新的收益。另外,通过外部渠道还可以整合其他行业的资源,利用移动智能终端给予用户随身

性的便捷,将极大地增加边际效益。目前常见的银行外部产品应用类型包含移动银行、移动掌上生活、移动理财投资、移动支付。常见的移动银行 App 如图 3-29 所示。



图 3-29 常见的移动银行 App

2. 移动支付

移动支付是指交易双方为了某种货物或者服务,使用移动终端设备为载体,通过移动通信网络实现的商业交易。移动支付所使用的移动终端可以是手机、PDA、移动 PC 等。移动支付的产业链如图 3-30 所示。

3. 移动证券

移动证券就是通过基于移动通信网络数据传输功能的新一代无线应用炒股系统,使普通手机成为一个综合处理终端。只要手机在 GSM(Global System for Mobile communication, 全球移动通信系统)/CDMA 网络覆盖范围内(可以接收信号),就可以查看股市行情、线路图等,掌控丰富的股市资源。与电话委托的“阻塞列表”和网络上的“线路不能连接”相比,移动电话在下单速度和线路畅通的可靠性上都更胜一筹。因此,目前除了柜台、电话委托和网上这三种方式外,最受股民欢迎的方式就是使用快捷、方便的手机委托交易了。常见的移动证券 App 如图 3-31 所示。

4. 移动保险

移动保险是指保险企业采用移动网络来开展一切活动的经营方式,它包括在保户、政府及

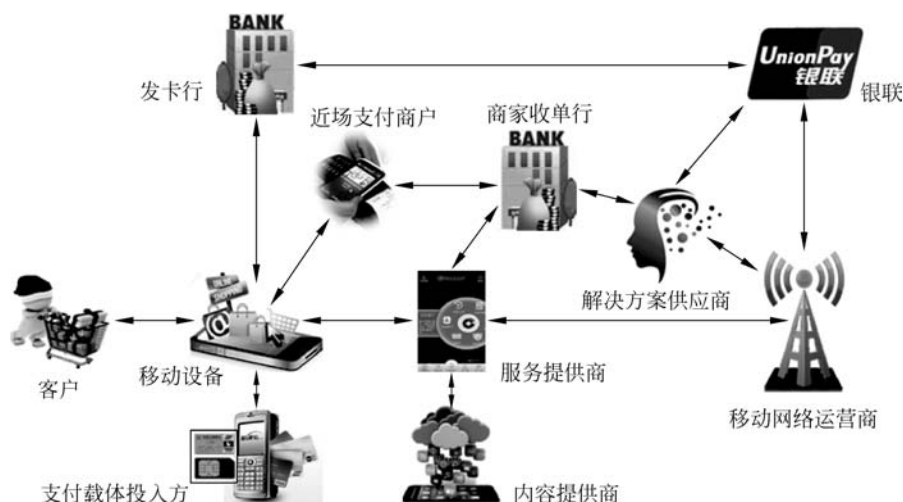


图 3-30 移动支付产业链



图 3-31 常见的移动证券 App

其他参与方之间通过移动设备来共享结构化和非结构化的信息,并完成商务活动、管理活动和消费活动。常见的移动保险 App 如图 3-32 所示。



图 3-32 常见的移动保险 App

移动保险的最终目标是实现电子交易,即通过移动网络实现投保、核保、理赔、给付。具体来讲,移动保险的应用范围主要包括以下几个方面。

(1) 移动报价

保险公司和一些分支机构将公司简介、公司险种、承保说明、服务内容等公司信息进行发布,让用户通过终端设备可以方便快捷地进行浏览、查询。

(2) 移动咨询

保险公司可以通过移动网络来实时解答客户提出的各种保险问题,宣传保险知识。保险公司可以随时以短信等方式向客户传递有关保险的各种信息。

(3) 移动投保

只要投保人将自己的姓名、性别、年龄、职业及需求保险意向等信息输入到保险公司的移动网络上,保险公司的网络系统就会自动从保险产品中为投保人设计一种最佳的保险计划。如果获得投保人同意,即可以完成一份移动投保单,如果保险公司同意承保,即可以通过短信或电子邮件方式予以确认。当保险费通过移动银行划入保险公司后,该份保险合同即可生效。

3.6 物联网技术

物联网面向实体世界,对实体世界进行追踪历史、把控现在、预测未来,改变了实体产业本身。物联网对传统产业的变革将远远超过互联网的影响,对金融领域的影响也将是广泛和深远的。物联网以其全新的架构体系,正在催生一种全新的金融模式——物联网金融。

3.6.1 物联网概述

物联网是通过射频识别、红外感应器、全球定位系统、激光扫描器等信息传感设备,按约定的协议,把任何物品与互联网相连接,进行信息交换和通信,以实现物品的智能化识别、定位、跟踪、监控和管理的一种网络。如图 3-33 所示。

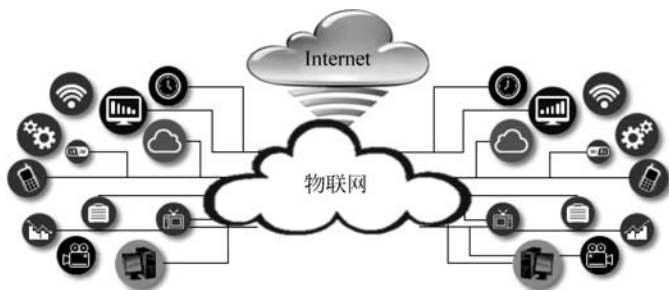


图 3-33 物联网示意图

物联网即“万物互联的互联网”,是在互联网基础上延伸和扩展的网络,它将各种信息传感设备与互联网结合起来而形成的一个巨大网络,实现在任何时间、任何地点,人、机、物的互联互通。

物联网是新一代信息技术的重要组成部分,IT 行业又称之为“泛互联”,意指物物相联,万物互联。由此,“物联网就是物物相连的互联网”。这里有两层意思:第一,物联网的核心和基础仍然是互联网,是在互联网基础上的延伸和扩展的网络;第二,其用户端延伸和扩展到了任何物品与物品之间,进行信息交换和通信。

物联网作为继计算机、互联网后信息产业革命的第三次浪潮,早已渗透到社会生产经营的方方面面,更是对社会、经济中枢的金融行业产生深远影响。金融物联网是指物联网技术在金融行业的全部应用。从一项或一组物联网技术对金融企业的内部管理支持和流程优化,到完整的物联网商业应用场景与金融企业具体业务的结合,再到多维度、全链条的智慧网络建设及数据应用推动的金融模式变革与创新,显示出巨大的威力。物联网技术在金融领域的应用不断深化,也带动相关产业呈现出强劲的发展势头。

金融机构利用以物联网为核心的信息技术,进行金融信用、杠杆、风险和服务的创新,从而深刻变革银行、证券、保险、租赁、投资等众多金融领域的原有业务模式。其中,物联网技术对于金融信用体系的创新,体现在金融机构在物联网技术支撑下,重构其与监管部门、非金融企业、服务对象等相关参与者之间的新型信用体系;物联网技术对于金融资本杠杆的创新,体现在金融机构通过构建物联网技术应用场景来引导更多的参与者投入实体经济,推动单一的金融资本杠杆向多样性的资本、技术等资源组合杠杆的转变;物联网技术对于金融风险管理的创新,体现在金融机构通过共享实体经济的物联网数据信息,实现智能客观的风险定价;物联

网技术对于金融产品服务的创新,体现在金融机构利用物联网技术实时地获取客观的市场需求,进而动态地调整金融服务,推动被动的融资服务向主动的融资融智服务转变。

金融物联网包含了物联网技术、金融服务以及实体经济的生产运营场景等基本要素。其中,金融和物联网技术是金融物联网的两个核心要素,相辅相成,互为支持;而实体经济的生产运营场景则是金融物联网的现实载体,金融服务与物联网技术在其中作为基础要素融入实体经济的商品或服务中。金融物联网构成的新型生产关系,因其高度的开放、协作以及全面的去中介化,使得信用、跨期价值交易的成本无限下降,产品服务边际成本趋近于零,业态边界也将趋于无穷大,可以扩张到所有的社会生活、生产和运营中,甚至囊括了所有的商业和非商业参与者。

3.6.2 物联网的关键技术

1. 物联网技术框架

从技术的角度来说,物联网技术主要有四个层面,如图 3-34 所示。



图 3-34 物联网技术框架

(1) 感知层

第一层是感知层,就是“物”的层面,此层面包含传感器、网关、终端硬件等。物联网的数据在这个层面从各种设备中被感知和产生。

(2) 网络层

第二层是网络层。各种物理设备,通过各种方式进行组网,形成了物联网的初级形态。

(3) 平台层

第三层是数据采集和分析层,也称平台层。数据在第三层中被集中采集到一个计算中心,通常是云计算平台,进行数据整理和计算,从而得到有用的分析结果。可以说第三层是物联网的灵魂。

(4) 应用层

第四层是分析结果的展现和应用。这一层完成物联网结果的反馈和与其他系统的对接,给生产、生活带来实质帮助。以上 4 个层面组成了在各行各业实现物联网方案的基本技术框架。

2. 物联网的关键技术

物联网可以将物体的信息上传到互联网,这项功能的实现主要依赖 3 项核心技术:射频识别技术、传感器技术和嵌入式系统技术。

(1) 射频识别技术

射频识别技术可以读取每个物体的“身份证”(RFID 标签)。即通过射频识别技术对物体属性进行标志,属性包括静态属性和动态属性,静态属性可以直接存储在 RFID 标签中,动态属性需要先由传感器实时探测。

(2) 传感器技术

传感器技术能将射频识别技术采集到的“身份信息”(模拟信号)转化为适合网络传输的数字电信号,再通过计算机进行数据处理。

(3) 嵌入式系统技术

嵌入式系统技术是综合了计算机软硬件、传感器技术、集成电路技术、电子应用技术为一体的复杂技术,可将物体的信息通过网络传输到信息处理中心,再由处理中心完成物体通信的相关计算,并发出各种指令。

3.6.3 金融物联网发展情况

当前物联网产业进入了飞速发展阶段,金融物联网应用方案逐步丰富,相应金融业务模式渐成体系。物联网技术与金融的结合,涉及银行、保险、融资租赁等多个业务方向,既有对这些机构内部运营管理的提升,也有金融模式的创新。

1. 物联网技术在金融企业内部运营管理的应用

目前,物联网在金融企业运营管理方面的应用从功能上主要可以分为两个维度。

(1) 提高企业内部管理能力

物联网感知设备能够实时不间断地对物体状态信息进行反馈,对金融企业的安全防卫、突发事件反应、提升内部运营效率等提供了很好的帮助。例如,RFID 银行运钞箱管理系统采用远距离射频感应技术,通过安装在运钞箱的电子标签与安装在金库的读写器之间的射频通信,记录和管理运钞箱出入金库的业务流程,通过网点的手持便携设备,记录和管理各个营业网点的运钞箱,实现了银行运钞箱在金库与营业网点间的自动化管理,提高了银行运钞箱管理效率与安全性,提升了银行的综合竞争力。

另外,金融物联网还能提升金融企业内部重要资料的管理能力,比如部分银行和保险公司采取的档案盒电子标签,不但可以实现业务进度查询、处理意见读写和流程时效管理,还能的内部服务计价、风险追责等提供佐证。

(2) 提升服务质量和客户体验

物联网信息的传送是建立在物与物之间,减少了人为的影响,对保障金融信息传输安全有很好的效果。例如,集成电路卡(IC 卡)、移动支付的兴起以及指纹、虹膜支付的逐步应用都是物联网技术在金融支付安全领域的应用体现。物联网不但保障信息传输的安全,还可以利用感知设备收集的真实数据集,延伸出更多的、特色化的应用形式,极大地提升金融企业的客户

体验。例如,远程开卡机通过摄像等读取设备提高了客户开卡的效率;微软研发的金融产品信息桌通过物联网技术可以智能地向客户展示金融产品信息及提供更多金融服务资讯,客户甚至可以在信息桌上完成金融产品或服务的购买。

2. 物联网技术与供应链金融业务的结合

物联网技术在帮助不同产业优化升级的过程中,发展出来的管理功能和数据信息可以帮助金融企业优化风险管理、简化业务操作流程,并推动产品创新。RFID、智能视频、工业二维码等物联网技术能够对商品流转、仓储进行实时的识别、定位、跟踪、监控等系统化、智能化管理,使得金融机构能够从时间、空间两个维度全面感知和监控动产的存续状态和变化过程,有效地提升了供应链金融业务风险管理和操作效率。

(1) 物联网在汽车供应链金融中的应用

平安银行依托自身在汽车供应链金融领域的优势,在“车厂—供应商”供应链融资环节,引入了物联网传感系统和智能监管系统,开创了物联网技术下“智能监管库存融资”模式,实现了技术监管对人工现场监管的优化升级、银行信贷业务模式的重塑和优化,极大地降低了人力成本和道德风险,并为银行风险管理提供了强劲的大数据支撑。

(2) 大宗商品动产融资

银行与大型港口、公共仓库等仓储物流企业建立战略合作,采用智能仓储监管方案,对钢铁、有色、石油、化工等大宗商品仓库进行物联网改造升级,实现对动产融资业务项下抵、质押物的实时动态监管,赋予动产以不动产的属性,囊括静态仓储和动态物流中的大宗商品,真正激活交易商品的金融属性。

(3) 交易见证及配套金融服务

伴随商品交易线上化的全面普及,贸易真实性问题成为限制交易配套金融服务发展的主要因素。电子交易平台、仓储物流企业、金融机构等应用物联网技术将线上信息化交易过程与线下商品实物的交割连接在一起,使得商品交易、实物交割与金融机构的资金监管、支付清算等服务匹配,达到交易信息流、物流和资金流的统一。

将RFID、重力感应器等物联网设备应用在高价值类商品的仓储物流中,可以实时读取线下交易商品品名、规格及数量等信息,准确监测货物的库存和物流状态,并将物联网化的仓储、物流信息系统与线上交易信息系统直连,为买卖双方动态掌控交易商品类别、快速判断交易时机提供了有效支撑,由此配置的交易见证、支付结算及供应链融资等金融服务也顺势得到了很好的发展。

(4) 仓单认证、交易及配套金融服务

由于近年来的虚假仓单、重复质押及监管过失等问题使仓单的交易及融资陷入了发展困境,频发的风险事件在影响行业信用体系的同时,也影响了商品交易的活跃度。交易市场、交割仓库、期货公司及银行等应用物联网技术将大宗商品实物与电子仓单绑定,使得仓单信息能根据实物的物理变动、权属变化等进行实时调整,并用套期保值交易锁定仓单价值,进而实现大宗商品实物交易及融资的单证化和线上化。

目前已有多家机构在进行仓单物联网化的研究和推动工作,其中有仓储机构、有大宗商品核心厂商,也有一些其他第三方机构,都致力于通过互联网、物联网及大数据等新兴技术,对仓单及其线下货物的相关信息进行动态、持续、统一地登记公示,逐步形成了集仓单认证、仓单征信、仓单保险、仓单交易及投融资于一体的仓单服务方案。

3. 物联网技术与保险的结合

对保险业来讲,精算最大的困难是无法获得准确全面的风险数据,物联网技术的应用和普及,将深刻地改变保险业态,让消费者更受益的精准定价保险产品时代已经开始萌芽,实时核保、实时定价等新技术应用,将使“一车一价”车险、带病投保健康险、弹性保额重疾险、防误导销售等变得可行。

平安产险、百度与车载诊断系统(On-Board Diagnostic, OBD)制造商元征科技公司在车联网保险方面建立了合作,共同推出基于 OBD 与位置服务(Location Based Service, LBS)技术的车联网智能硬件——百度地图版(Golo),通过对车主行驶数据的持续分析,为其提供便捷、快速、个性化的车险服务,并通过与汽车产业链上各方参与者的信息共享,围绕汽车的“买、卖、养、用、玩”等场景,提供汽车按揭、安全咨询、加油、洗车等多元化服务。

此外,针对个人的寿险和健康险方面,保险行业也已开始尝试运用物联网技术,并催生出新的商业价值。例如,众安保险推出的一款基于日常慢跑的重疾险产品,就是将客户每天慢跑达标情况与保费优惠结合起来。这一看似简单的变革,却是保险精算传统的一大突破,改变了传统保险产品固定费率、固定保障、无法细分人群的旧模式,极大地提升了客户体验和实效。

本章小结

金融电子商务的 IT 技术背景除了传统的计算机、网络 and 现代金融设备外,大数据、云计算、区块链、人工智能、移动互联网、物联网等新一代信息技术正在与金融行业不断整合,并促使金融电子商务向纵深发展。大数据指无法在一定时间范围内用常规软件工具进行捕捉、管理和处理的数据集合,是需要新处理模式才能具有更强的决策力、洞察发现力和流程优化能力的海量、高增长率和多样化的信息资产;大数据具有大量、多样、高速、可变、真实、价值等特征;随着大数据技术的快速发展,大数据在金融业的应用场景正在逐步拓展,在风险控制、运营管理、销售支持和商业模式创新等细分领域都得到了广泛的应用。云计算是由分布式计算、并行处理、网络计算发展而来的,是一种新兴的商业计算模式;云计算经历了电厂模式、效用计算、网络计算和云计算 4 个阶段;云计算具有大规模、分布式、虚拟性、可用性、扩展性、个性化、低成本、安全性等特点;云计算使用了许多技术,其核心技术有编程模型、海量数据分布存储技术、海量数据管理技术、虚拟化技术和云计算平台管理技术;当前,云计算已引发金融领域重大变革,是金融科技的重要组成部分。区块链技术是指通过去中心化和去信任的方式集体维护一个可靠分布式共享数据库的技术方案,是构建去中心化可信环境的基础协议;去中心、去中介是区块链最本质的特征;区块链技术所解决的问题可用 4 个字概况:“记账”+“认账”;“记账”的方式采用分布式,包括分布式记账、分布式传播和分布式存储;“认账”的方式采用去中心机制+共识机制;区块链用到的核心技术包括“区块+链”的数据结构、开源去中心化协议、非对称加密技术和智能合约;区块链技术在金融领域的应用包括数字货币、数字票据、跨境支付、数字资产、金融交易、融资众筹、供应链金融、互助保险、按揭业务等。人工智能是一门研究、开发用于模拟、延伸和扩展人的智能的理论、方法、技术及应用系统的新技术科学;人工智能的发展几经波折,在 21 世纪大数据和云计算技术发展之后才逐渐走上正轨,其主要的应用领域包括计算机视觉、自然语言处理、智能机器人等;人工智能主要面临 3 个问题:计算机博弈的困难、理论的不成熟以及模式识别的困惑。金融电子商务的兴起得益于互联网技术,金融电子商务的普及则得益于移动通信技术,得益于智能手机的普及,得益于移动

互联网技术。移动互联网是指用户可以使用手机、笔记本电脑等移动终端,通过协议接入互联网;移动互联网在金融领域的应用包括移动银行、移动支付、移动证券、移动保险等。物联网是通过射频识别、红外感应器、全球定位系统、激光扫描器等信息传感设备,按约定的协议,把任何物品与互联网相连接,进行信息交换和通信,以实现物品的智能化识别、定位、跟踪、监控和管理的一种网络;物联网技术框架包括感知层、网络层、平台层和应用层,其核心技术包括射频识别技术、传感器技术和嵌入式系统技术;物联网技术与金融的结合,涉及银行、保险、融资租赁等多个业务方向,既有对这些机构内部运营管理的提升,也有金融模式的创新。



案例阅读