公共素质课精品系列规划教材

扫描二维码
共享立体资源

医学计算机基础

YIXUE JISUANJI JICHU

主　审　刘瑛贵
主　编　张　华　司　洁

北京出版集团
北京出版社

医学计算机基础
主审 刘瑛贵 主编 张华 司洁
北京出版集团 北京出版社

图书在版编目（CIP）数据

医学计算机基础 / 张华，司洁主编 . — 北京 : 北京出版社，2020.10（2022 重印）

ISBN 978-7-200-15994-3

Ⅰ. ①医… Ⅱ. ①张… ②司… Ⅲ. ①计算机应用—医学—高等职业教育—教材 Ⅳ. ① R319

中国版本图书馆 CIP 数据核字（2020）第 209155 号

医学计算机基础

YIXUE JISUANJI JICHU

主　　编：张　华　司　洁

出　　版：北京出版集团

　　北京出版社

地　　址：北京北三环中路 6 号

邮　　编：100120

网　　址：www.bph.com.cn

总 发 行：北京出版集团

经　　销：新华书店

印　　刷：定州启航印刷有限公司

版 印 次：2020 年 10 月第 1 版　2022 年 8 月修订　2022 年 8 月第 2 次印刷

成品尺寸：185 毫米 ×260 毫米

印　　张：17.5

字　　数：383 千字

书　　号：ISBN 978-7-200-15994-3

定　　价：56.00 元

教材意见建议接收方式：010-58572162　邮箱：jiaocai@bphg.com.cn

如有印装质量问题，由本社负责调换

质量监督电话：010-82685218　010-58572162　010-58572393

目录

单元一

计算机与信息技术

学习目标

1. 了解计算机的发展简史。
2. 掌握进制数之间的转换方法。
3. 掌握计算机系统的组成。
4. 了解计算机和网络新技术。
5. 熟悉计算机病毒的概念及预防。

计算机发展与基础知识

第一节 如何将计算思维引入大学生计算机课程

一、计算思维的概念

美国卡内基·梅隆大学周以真教授提出，计算思维（Computational Thinking，CT）是运用计算机科学的基础概念去求解问题、设计系统和理解人类行为等，涵盖了计算机科学广度的一系列思维活动。

计算思维的详细描述如下。

计算思维就是通过约简、嵌入、转化和仿真等方法，把一个看起来困难的问题重新阐释成一个人们知道问题怎样解决的思维方法。计算思维是一种递归思维，是一种并行处理，能把代码译成数据，又能把数据译成代码，是一种多维分析推广的类型检查方法。计算思维是一种采用抽象和分解的方法来控制庞杂的任务或进行巨大复杂系统设计的方法，是一种基于关注点分离的方法。计算思维是选择合适的方式去陈述一个问题，或对一个问题的相关方面建模使其易于处理的一种思维方法。计算思维是按照预防、保护及通过冗余、容错、纠错的方式，并从最坏情况进行系统恢复的一种思维方法。计算思维是利用启发式推理寻求解答，即在不确定情况下的规划、学习和调度的思维方法。计算思维是利用海量数据来加快计算，在时间和空间之间，在处理能力和存储容量之间进行折中的思维方法。

二、计算思维的特征

（一）是概念化而不是程序化

计算机科学不仅仅是计算机编程。像计算机科学家那样去思维意味着远远不仅限于计算机编程，还要求能够在抽象的多个层次上进行思维。计算机科学不只是关于计算机，就像音乐不只是关于麦克风一样。

（二）是根本的而不是刻板的技能

计算思维是一种根本技能，是每个人为了在现代社会中发挥职能所必须掌握的。刻板的技能意味着简单的机械重复。

（三）是人的思维而不是计算机的思维

计算思维是人类求解问题的一条途径，但绝非要使人类像计算机那样思考。计算机枯燥且沉闷，人类聪颖且富有想象力，是人类赋予了计算机激情。计算机赋予人类强大的计算能力，人类应该好好利用这种力量去解决各种需要大量计算的问题。

（四）是思想而不是人造物

计算思维不只是将硬件和软件等人造物以物理形式呈现给人们，更重要的是计算的概念，这种概念被人们用于求解问题、管理日常生活以及与他人进行交流和互动。

（五）数学和工程思维的互补与融合

计算机科学在本质上源自数学思维，其形式化基础是建筑于数学之上的。计算机科学又从本质上源自工程思维，因为人们建造的是能够与实际世界互动的系统，基本计算设备的限制迫使计算机科学家必须计算性地思考，而不能只是数学性地思考。所以计算思维是数学和工程思维的互补与融合。

（六）面向所有人和所有地方

当计算思维真正融入整个人类活动时，它作为一个问题求解的有效工具，人人都应当掌握，处处都会被使用。

三、计算思维的应用领域

尽管计算思维被冠以计算两个字，但它绝不是只与计算机科学有关的思维，而是人类科学思维的一个远早于计算机出现的组成部分。只是由于计算机的发展极大地促进了对这种思维的研究和应用，并且这种思维在计算机科学的研究和工程应用中得到了广泛的认同，所以人们习惯地叫作计算思维。

计算思维代表着一种普遍的认识和一类普适的技能，它应该像“读、写、算”一样成为每个人的基本技能，而不仅仅限于计算机科学家，因此，每个人都可以尝试计算思维的学习和应用。计算思维这一领域提出的新思想、新方法将会促进自然科学、工程技术和社会经济等领域产生革命性的研究成果，计算思维也是创新人才的基本要求和专业素质。

数据在计算机中的表示

第二节　计算机系统组成及其工作原理

一、计算机工作原理

从第一代计算机发展到现在，计算机制造技术发生了天翻地覆的变化，但就其工作原理和体系结构而言，仍然在使用“计算机之父”冯·诺依曼于 1945 年提出的存储程序和程序控制的思想体系，即把程序和数据存储在存储器内，由控制器根据程序中的一系列指令进行计算。他的主要设计思想可以归纳为以下三点。

（1）计算机内部采用二进制形式表示数据和指令。

（2）确定计算机由运算器、控制器、存储器、输入设备和输出设备五个部件组成，并指明各自的功能和它们之间的联系。

（3）程序和指令存放在存储器中，计算机工作时无须人为干预，它会自动逐条地从存储器中调取指令并执行。

二、微型计算机系统的组成

微型计算机系统包括硬件系统和软件系统两大部分，二者缺一不可。

（一）微型计算机的硬件系统

1. 中央处理器（CPU）

中央处理器（CPU）主要包括运算器（ALU）和控制器（CU）两大部件。此外，还包括若干个寄存器和高速缓冲存储器。它是计算机的核心部件，又称微处理器，它的品质在很大程度上决定了整台计算机的速度和性能。计算机的所有操作都受 CPU 控制，CPU、主板和内存储器构成了计算机的主机，是计算机系统的主体。Intel 公司生产的 i9 系列 CPU 如图 1-1 所示。

图 1—1　Intel 公司 CPU

目前微型计算机的 CPU 生产商主要为 Intel 公司和 AMD 公司。1971 年，Intel 公司发布了世界上第一块微处理器 Intel4004，随后又不断推出了 80 系列、Pentium 系列、酷睿系列；AMD 公司起初推出的 AM2900 系列，到后来的 k5、k6、k7、Athlon64 系列，CPU 的复杂度、尺寸、结构与形态在这几十年间都在不断变化，功能也越来越强大。CPU 的发展始终遵循着摩尔定律。

CPU 的主要性能指标有时钟主频、字长、核心数。

（1）时钟主频。

时钟主频是指 CPU 的时钟频率，是微型计算机性能的一个重要指标，它的高低在一定程度上决定了计算机速度的快慢。主频以吉赫兹（GHz）为单位，一般来说，主频越高，速度越快。

（2）字长。

字长是指计算机部件一次能同时处理的二进制数据的位数。字长的大小决定了计算机的运算速度，字长越长，所能处理的数的范围越大，运算精度越高，处理速度越快。

（3）核心数。

一块 CPU 基板上集成多颗处理器的核心，通过并行总线将各处理器核心连接起来，变成多核心处理器的方式成为提高 CPU 性能的重要途径。目前的市场上多核 CPU 主要有双核、三核、四核、六核和八核 CPU。

2. 存储器

计算机的存储器分为两大类：一类是设在主机中的内部存储器，也叫主存储器，用于存放当前运行的程序和程序所用的数据，属于临时存储器；另一类是属于计算机外部设备的存储器，叫外存储器，简称外存，也叫辅助存储器，简称辅存。外存中存放暂时不用的数据和程序，属于永久性存储器，当需要时应先调入内存。

（1）主存储器。

①内存储器。

内存储器分为随机存储器（RAM）和只读存储器（ROM）两类。

A. 随机存储器（RAM）。随机存储器也叫读写存储器。其特点是存储的信息既可以读出，又可以向内写入信息，断电后信息全部丢失。随机存储器又可以分为静态 RAM 和动态 RAM 两种。

静态 RAM 的特点是只要不断电，信息就可长时间保存。其优点是速度快，不需要刷新，工作状态稳定；缺点是功耗大，集成度低，成本高。

动态 RAM 的优点是使用组件少，功耗低，集成度高；缺点是存取速度较慢且需要刷新。

B. 只读存储器（ROM）。只读存储器的特点是存储的信息只能读出，不能写入，断电后信息不会丢失。只读存储器大致可分成三类：掩膜型只读存储器（MROM）、可编程只读存储器（PROM）和可擦除的可编程只读存储器（EPROM）。

关于 RAM 和 ROM 之间，以及动态 RAM 和静态 RAM 之间的区别，如表 1-1 所示。

表 1-1　内存分类及对比

<table>
<tr><th rowspan="2">内存类型</th><th colspan="3">静态 RAM 和动态 RAM 的区别</th><th rowspan="2">RAM 和 ROM 的区别</th></tr>
<tr><th>区别点</th><th>静态 RAM</th><th>动态 RAM</th></tr>
<tr><td rowspan="4">随机存储器（RAM）</td><td>1</td><td>集成度低</td><td>集成度高</td><td rowspan="4">信息可以随时写入写出。写入时，原数据被冲掉。加电时信息完好，一旦断电，信息消失，无法恢复</td></tr>
<tr><td>2</td><td>价格高</td><td>价格低</td></tr>
<tr><td>3</td><td>存取速度快</td><td>存取速度慢</td></tr>
<tr><td>4</td><td>不需要刷新</td><td>需要刷新</td></tr>
<tr><td>只读存储器（ROM）</td><td>分类</td><td colspan="2">可编程只读存储器（PROM）、可擦除的可编程只读存储器（EPROM）、掩膜型只读存储器（MROM）</td><td>信息是永久性的，即使关机也不会消失</td></tr>
</table>

②高速缓冲存储器（Cache）。

CPU 的速度越来越快，但是内存的速度受到制造技术的限制无法同步 CPU，因而导致 CPU 不得不降低速度来适应内存。为了协调 CPU 和内存之间的速度差，通常在 CPU 和主存储器之间安装一个小而快的存储器，被称为高速缓冲存储器（Cache）。Cache 按其功能通常分为两类：CPU 内部的 Cache 和 CPU 外部的 Cache。

CPU 内部的 Cache 也称为一级 Cache，它是 CPU 内核的一部分，负责 CPU 内部的寄存器与外部的 Cache 之间的缓冲。

CPU 外部的 Cache 是二级 Cache，它相对于 CPU 是独立的部件，主要用于弥补 CPU 内部 Cache 的容量，负责整个 CPU 与内存之间的缓冲。

③内存储器的性能指标。

存储器的主要性能指标有两个：容量和速度。

容量指一个存储器包含的存储单元数，一般以字节为单位，如 8 KB、128 MB、4 GB 等。存储器的容量对一台计算机的整体性能指标具有重要的影响，容量越大，保存的信息越多，处理问题的能力也就越强。速度是衡量存储器性能的另一个重要指标，一般用存储周期（也称读写周期）来表示。存储周期指 CPU 从内存储器中读取数据所需的时间。

（2）外存储器。

外存储器也叫作辅助存储器，是指除计算机内存和中央处理器缓存以外的存储器。与内存相比，这类存储器的特点是存储容量大、价格较低，而且在断电后也可以长期保存信息，所以又称为永久性存储器。比较常见的外存储器有硬盘、光盘与光驱和U盘。

①硬盘。

硬盘是计算机的主要存储设备，磁盘驱动器和盘片都是固定于机箱内。计算机的硬盘技术发展十分迅速，从若干年前的几十兆、几百兆发展到现在的上千个G字节，现代硬盘容量几乎都是以T为单位。

磁盘的存储容量可用如下公式计算：

存储容量 = 磁道数 × 扇区数 × 扇区内字节数 × 面数 × 磁盘片数

②光驱与光盘。

光驱是用来读写光盘内容的设备，是计算机中比较常见的硬件设备。

常用的光驱分为如下几类。

A. CD-ROM光驱：又称为致密盘只读存储器，是一种只读的光存储介质。它是利用原本用于音频CD的格式发展起来的。价格便宜，但只能读容量很小的CD盘。

B. DVD光驱：一种可以读取DVD碟片的光驱，兼容性较好。价格适中，在兼容读CD盘的情况下，还可用来读大容量的DVD盘。

C. 刻录光驱：包括了CD和DVD的刻录机功能，外观和普通光驱相似，但前置面板清楚标识着写入、复读和读取的速度。价格略高，除了拥有DVD-ROM的功能外，还可以自己刻录CD盘、DVD盘。

光盘是一种新型的大容量辅助存储器，呈圆盘状，与磁盘类似，需要光盘驱动器来读写。它不是用电磁转换的机制读写信息，而是用光学的方式进行的。常见的光盘存储器分为如下几类。

A. CD光盘存储器。

第一类是只读型光盘CD-ROM。与ROM类似，即光盘中的数据由生产商预先写入，用户只能读取数据而不能修改。这类光盘现在被广泛应用。

第二类是一次性写入光盘CD-R。这类光盘用户可以写入，但只能写入一次，一旦写入，可多次读取。

第三类是可擦除型光盘CD-RW。其存储功能与磁盘相似，用户可以多次对其进行读/写。

B. DVD光盘存储器。

DVD光盘与CD光盘大小相同，但它存储密度高，单面光盘可以分单层或双层存储信息，一张光盘有两面，最多可以有4层存储空间，所以存储空间极大。120 mm的单面单层DVD光盘的存储容量为4.7 GB。目前常用的DVD光盘分为DVD-ROM、DVD-R、DVD-RW、DVD-Video和DVD-Audio等5类。

C. 蓝光光盘存储器。

蓝光光盘存储器（Blu-ray Disc，BD）是一种最新的革命性存储技术，多用于PC

产品、消费性电子产品和游戏机。它可以录制、重复写入及播放高清画质的影片，也可以存储大容量的数据资料。为更高品质的光影存取，提供划时代的新体验。Blu-ray Disc 可以存储 25 GB 的数据与单层的光盘面，单面双层的存储容量可达到 50 GB。

光盘的特点如下。

一是存储容量大，价格低。

二是不怕磁性干扰，光盘比磁盘的记录密度更高、更可靠。

三是存取速度快，目前主流光驱为 50 倍速和 52 倍速。

③ U 盘。

U 盘又称为 USB 盘或者拇指盘。它利用闪存在断电后还能保持存储数据而不丢失的特点而制成，非常适合复制文件及数据交换的应用。其优点是重量轻、体积小，一般只有拇指大小，15 ～ 30 g 重，通过计算机的 USB 接口即插即用，使用方便，存储容量一般为 8 GB、16 GB、32 GB 不等。U 盘可以分为基本型、增强型和加密型三种类型。

3. 总线和主板

所谓总线（Bus）就是系统部件之间传送信息的公共通道，各部件由总线连接并通过它传递数据和控制信号。常见的总线标准有 ISA 总线、PCI 总线、AGP 总线和 EISA 总线等。

总线体现在硬件上就是计算机的主板（Main Board），它也是配置计算机的主要硬件之一。主板上配有插入 CPU、内存条、显示卡、声卡、网卡、鼠标器和键盘器等部件的各类扩展槽或接口，而光盘驱动器和硬盘驱动器则通过电缆与主板连接。主板的性能影响着整个计算机的性能。

一个基于总线结构的计算机结构示意图如图 1-2 所示。

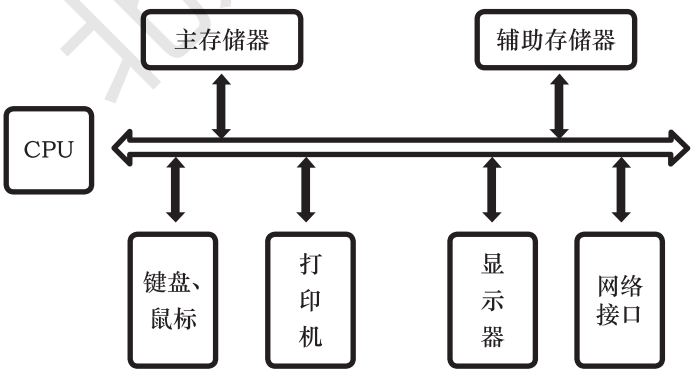

图 1-2　基于总线结构的计算机结构示意图

4. 输入设备

（1）键盘。

键盘是用户与计算机进行交流的主要输入工具，是输入文字最方便的工具。键盘的每一个按键相当于使对应按键的机械开关闭合，产生一个信号，由键盘电路进行编

码输入到计算机进行处理。

传统的键盘是机械式的，通过导线与计算机相连。通常使用的键盘有 104 键盘、107 键盘、人体工程学键盘、多媒体键盘、无线键盘等。键盘接口的规格有 PS/2 和 USB 两种。

（2）鼠标。

鼠标又称鼠标器，通常有两个按键和一个滚轮，当它在平板上滑动时，屏幕上的指针也跟着移动。目前，鼠标在多窗口环境下，更是一种必不可少的输入设备。

常见的鼠标有机械鼠标、光学鼠标和光学机械鼠标。为了操作和携带方便，无线鼠标已经得到了广泛的应用。

（3）其他输入设备。

计算机中常用的输入设备除了键盘和鼠标以外，还有扫描仪、手写输入设备、声音输入设备、触摸屏和条形码阅读器等设备。现在的输入设备种类越来越多，而且越来越接近人类的器官。

5. 输出设备

（1）显示器。

显示器又称监视器，是计算机最重要的输出设备之一，也是人机交互必不可少的设备。显示器显示的信息不再是单一的文本和数字，也可以显示图形、图像和视频等多种不同的信息。

常用的显示器有阴极射线管显示器（简称 CRT）和液晶显示器（简称 LCD）两种。CRT 显示器又有球面和纯平之分。液晶显示器因为其体积小、功耗低、发热小、辐射低等特性，已经逐步取代 CRT 显示器，成为市场中的主流。

显示器的性能指标如下。

①分辨率。分辨率指屏幕上每行有多少像素点、每列有多少像素点，一般用矩阵行列式来表示，其中每个像素点都能够被计算机单独访问。常用显示器的分辨率为 1 024 × 768 像素、1 152 × 864 像素、1 920 × 1 080 像素等。

②刷新率。刷新率指每个像素为该频率所刷新的时间，与屏幕扫描速度及避免屏幕闪烁的能力有关。刷新率过低，可能出现图像闪烁或抖动。

③显存。显存与电脑内存相似。显存越大，可以存储的像素数据就越多，支持的分辨率与颜色数也就越高。

④尺寸。尺寸以显示器的对角线来度量。目前常用的产品尺寸多为 17 英寸、19 英寸、22 英寸。

（2）打印机。

打印机用于将计算机中的文本、图像或报表等打印到纸上，属于计算机常用的外部设备之一。常见的打印机有点阵式打印机、喷墨式打印机和激光打印机三种。

（3）其他的输出设备。

常用的输出设备除了显示器和打印机外，还有绘图仪、音箱等向操作者提供输出

结果的设备。

6. 微型计算机的主要技术指标

（1）字长。一次能并行处理的二进制位数，如 8、16、32、64 位等。

（2）主频。计算机 CPU 的时钟周期，单位是兆赫兹（MHz）。

（3）运算速度。计算机每秒所能执行加法指令的数目。运算速度的单位是百万次 / 秒（MIPS）。

（4）存储容量。存储容量包括主存容量和辅存容量，主要指内存储器所能存储信息的字节数。

（5）存储周期。存储器进行一次完整的存取操作所需的时间。

（二）微型计算机的软件系统

软件系统是为运行、管理和维护计算机而编制的各种程序、数据及文档的总称。硬件系统和软件系统互相依赖、不可分割。

1. 进程与线程

（1）进程。进程是程序的一次执行过程，是系统进行调度和资源分配的一个独立单位。或者说，进程是一个程序与其数据一起在计算机上顺利执行时所发生的活动。

（2）线程。如果一个程序可以被分解为多个进程共同完成程序的任务，那么被分解的不同进程就叫作线程。

2. 软件系统及其组成

系统软件（System Software）和应用软件（Application Software）组成了计算机软件系统的两个部分（图 1-3）。

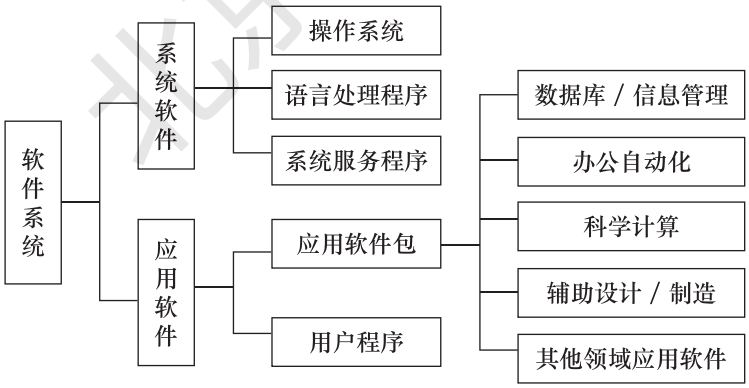

图 1-3　计算机软件系统的组成

3. 操作系统

操作系统是控制、管理计算机硬件资源和软件资源的大型系统软件，是计算机所有软、硬件系统的组织者和管理者，它能合理地组织计算机的工作流程，控制用户程序的运行，为用户提供各种服务。操作系统由许多具有控制和管理功能的子程序组成。典型的操作系统有 DOS、UNIX、Windows、OS/2、Linux、Android 等。

4. 语言处理程序

程序是人们为解决某一问题而为计算机编写的一组命令序列，是指令的有序集合。程序设计语言通常分为机器语言、汇编语言和高级语言三类。

（1）机器语言。机器语言是计算机唯一能够识别并直接执行的语言。机器语言中的每一条语句实际上都是二进制形式的指令代码。

（2）汇编语言。汇编语言采用一定的助记符号表示机器语言中的指令和数据。用汇编语言编写的程序称为汇编语言源程序。计算机不能直接识别它，必须先把汇编语言源程序翻译成机器语言程序（目标程序），然后才能被执行。

（3）高级语言。高级语言比较接近于人们习惯用的自然语言和数学表达式。高级语言要用翻译的方法把它翻译成机器语言程序才能执行。翻译的方法有“解释”和“编译”两种。一个高级语言源程序必须通过“编译”和“连接”才能成为可执行的机器语言。

5. 应用软件

常用的应用软件有如下几类。

（1）办公软件，如 Microsoft Office 和金山公司的 WPS 等。

（2）多媒体处理软件，如 Adobe 公司的 Photoshop 等。

（3）Internet 工具软件，如 Web 服务软件、Web 浏览器、文件传送工具 FTP、远程访问工具 Telnet、下载工具 Flash Get 等。

（4）杀毒软件，如金山毒霸、卡巴斯基、瑞星、诺顿、360 等。

第三节 计算机技术与网络技术的最新发展

虽然从第一台电子计算机诞生至今只过去了 70 多年的时间，但信息技术的发展速度和应用广度都是非常惊人的。尤其是进入 21 世纪后，在计算机、网络、通信这三个信息技术核心技术领域出现并成熟了一批新技术、新应用和新思维。本节主要介绍物联网、云计算、大数据技术、3D 打印技术、人工智能和区块链技术。

一、物联网

（一）物联网的概念

物联网是在互联网概念的基础上，将其用户端延伸和扩展到任何物品，进行信息交换和通信的一种网络概念。互联网时代，人与人之间的距离变近了；而物联网时代，则是人与物、物与物之间的距离变近了。物联网是全新的网络架构，可以实现全球范围内物品的跟踪和信息的共享，如图 1-4 所示。

物联网是指通过射频识别（RFID）、红外感应器、全球定位系统、激光扫描器、气体感应器等信息传感设备，按照约定的协议，把任何物品与互联网连接起来进行信息交换和通信，以实现智能化识别、定位、跟踪、监控和管理的一种网络。

图 1–4　物联网

物联网的英文名称是“The Internet of Things”。顾名思义，物联网就是物物相连的互联网。这里有两层意思：其一，物联网的核心和基础仍然是互联网，是在互联网基础上延伸和扩展的一种网络；其二，物联网用户端延伸和扩展到了任何物品，是任意物品之间进行的信息交换和通信。

（二）物联网体系架构

目前，业界一致认同的物联网体系架构是将其分为三个层次，底层是用来感知数据的感知层，中间是数据传输的网络层，最上面则是内容应用层。

在物联网体系架构中，三个层次的关系可以这样理解：感知层相当于人体的皮肤和五官；网络层相当于人体的神经中枢和大脑；应用层相当于人的社会分工，具体描述如下。

1. 感知层

感知层是物联网的皮肤和五官。感知层包括二维码标签和识读器、RFID 标签和读写器、摄像头、GPS 等，主要作用是识别物体，采集信息，与人体结构中皮肤和五官的作用相似。

2. 网络层

网络层是物联网的神经中枢和大脑。网络层包括通信与互联网的融合网络、网络管理中心和信息处理中心等，主要作用是将感知层获取的信息进行传递和处理，类似于人体结构中的神经中枢和大脑。

3. 应用层

应用层是物联网的“社会分工”。应用层是物联网与行业专业技术的深度融合，主要作用是与行业需求结合，实现行业智能化，这类似于人的社会分工，最终构成人类社会。

在各层之间，信息不是单向传递的，也有交互、控制等。各层所传递的信息是多

种多样的，这其中关键是物品的信息，包括在特定应用系统范围内能唯一标识物品的识别码和物品的静态与动态信息。

（三）物联网的应用领域

物联网用途广泛，遍及智能交通、环境保护、政府工作、公共安全、平安家居、智能消防、工业监测、老人护理、个人健康、花卉栽培、水系监测、食品溯源、敌情侦查和情报搜集等众多领域。展望未来，随着技术的不断进步，物联网将会成为人们生活的一部分。

物联网把新一代 IT 技术充分运用到各行各业之中。具体来说，就是把感应器嵌入和装备到电网、铁路、桥梁、隧道、公路、建筑、供水系统、大坝、油气管道等各种物体中，然后将物联网与现有的互联网整合起来，实现人类社会与物理系统的整合。在这个整合的网络当中，存在能力超级强大的中心计算机群，能够对整合网络内的人员、机器、设备和基础设施实施实时的管理和控制。在此基础上，人类可以以更加精细和动态的方式管理生产及生活，达到“智慧”状态，提高资源利用率和生产力水平，改善人与自然的关系。物联网描绘的是充满智能化的世界，在物联网的世界里万物都将相连，信息技术已经上升为让整个世界更加智能的智慧地球的新阶段。

二、云计算

（一）云计算的概念

云计算（Cloud Computing）概念是由 Google 在 2006 年提出的，是一种基于互联网的计算方式。狭义的云计算是指信息技术基础设施的交付和使用模式，指通过网络以按需、易扩展的方式获得所需的资源。广义的云计算是指服务的交付和使用模式，指通过网络以按需、易扩展的方式获得所需的服务。这种服务可以是和信息技术、软件、互联网相关的，也可以是任意其他的服务，它具有超大规模、虚拟化、可靠安全等特点。

（二）云计算的特点

1. 超大规模

“云”具有相当大的规模，Google 云计算已经拥有 100 多万台服务器，Amazon、IBM、微软和 Yahoo 等公司的“云”均拥有几十万台服务器。“云”能赋予用户前所未有的计算能力。

2. 虚拟化

云计算支持用户在任意位置使用各种终端获取服务。所请求的资源来自“云”，而不是固定的有形的实体。应用在“云”中某处运行，但实际上用户无须了解应用运行的具体位置，只需要一台笔记本或一部智能手机，就可以通过网络服务来获取各种服务。

3. 高可靠性

“云”使用了数据多副本容错、计算节点同构可互换等措施来保障服务的高可靠性，

使用云计算比使用本地计算机更加可靠。

4. 通用性

云计算不针对特定的应用，在“云”的支撑下可以构造出千变万化的应用，同一片“云”可以同时支持不同的应用运行。

5. 高可伸缩性

“云”的规模可以动态伸缩，满足应用和用户规模增长的需要。

6. 按需服务

“云”是一个庞大的资源池，用户按需购买，像使用自来水、电和煤气那样计费。

7. 极其廉价

“云”的特殊容错措施使得其可以采用极其廉价的节点来构成云；“云”的自动化管理使数据中心管理成本大幅降低；“云”的公用性和通用性使资源的利用率大幅提升；“云”设施可以建在电力资源丰富的地区，从而大幅降低能源成本。因此，用户可以充分享受“云”的低成本优势，需要时，花费几千元、一天时间就能完成以前需要数十万元、数月时间才能完成的数据处理任务。

（三）云计算机的应用

1. 云物联

云物联指的是在物联网行业加入云计算，直接以云服务平台为客服提供服务，从而提供更贴心的服务。

2. 云安全

云安全（Cloud Security）是一个从云计算演变而来的新名词。云安全的策略构想是使用者越多，每个使用者就越安全。因为如此庞大的用户群足以覆盖互联网的每个角落，只要某个网站被挂马或某个新木马病毒出现，就会立刻被截获。

云安全通过网状的大量客户端对网络中软件行为的异常进行监测，获取互联网中恶意程序的最新信息，推送到 Server 端进行自动分析和处理，再把针对恶意程序的解决方案分发到每个客户端。

3. 云存储

云存储是在云计算（Cloud Computing）概念上延伸和发展出来的一个新的概念，是指通过集群应用、网格技术或分布式文件系统等功能，将网络中大量不同类型的存储设备通过应用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一个系统。当云计算系统运算和处理的核心是大量数据的存储和管理时，云计算系统中就需要配置大量的存储设备，那么云计算系统就转变为一个云存储系统，所以云存储是一个以数据存储和管理为核心的云计算系统。

4. 云游戏

云游戏是以云计算为基础的游戏方式，在云游戏的运行模式下，所有游戏都在服务器端运行，并将渲染完毕后的游戏画面压缩后通过网络传送给用户。在客户端，用

户的游戏设备不需要任何高端处理器和显卡，只需要具有基本的视频解压能力就可以了。就现今来说，云游戏还没有成为家用机和掌机界的联网模式，因为至今 X360 仍然在使用 Live，PS 是 PS NETWORK，Wii 是 Wi-Fi。但是几年或十几年后，云计算取代这些东西成为其网络发展的终极方向的可能性非常大。

5. 云计算

从技术上看，大数据与云计算的关系就像一枚硬币的正反面一样密不可分。大数据必然无法用单台计算机进行处理，必须采用分布式计算架构。它的特色在于对海量数据进行挖掘，但它必须依托云计算的分布式处理、分布式数据库、云存储和虚拟化技术。

（四）云计算的服务类型

云计算按照服务类型大致可以分为三类：基础设施即服务（IaaS）、平台即服务（PaaS）和软件即服务（SaaS），如图 1-5 所示。

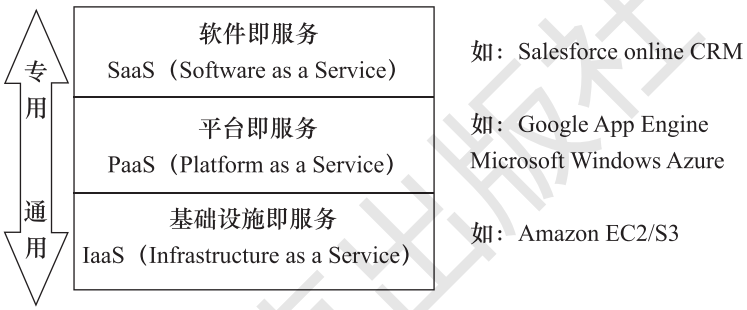

图 1-5　云计算的服务类型

1. 基础设施即服务（IaaS）

IaaS 将硬件设备等基础资源封装成服务，供用户使用，如亚马逊云计算 AWS（Amazon Web Services）的弹性计算云 EC2 和简单存储服务 S3。在 IaaS 环境中，用户相当于在使用裸机和磁盘，既可以让它运行 Windows，也可以让它运行 Linux，因而几乎可以做任何想做的事情，但用户必须考虑如何才能让多台机器协同起来工作。

2. 平台即服务（PaaS）

PaaS 对资源的抽象层次更进一步，它提供用户应用程序的运行环境，典型的如 Google App Engine。微软的云计算操作系统 Microsoft Windows Azure 可大致归入这一类。PaaS 自身负责资源的动态扩展和容错管理，用户应用程序不必过多考虑节点间的配合问题。但与此同时，用户的自主权降低，必须使用特定的编程环境并遵照特定的编程模型。

3. 软件即服务（SaaS）

SaaS 的针对性更强，它将某些特定应用软件功能封装成服务，如 Salesforce 公司提供的在线客户关系管理 CRM（Client Relationship Management）服务。SaaS 既不像 PaaS 一样提供计算或存储资源类型的服务，也不像 IaaS 一样提供运行用户自定义应用

程序的环境，它只提供某些专门用途的服务供应用调用。

需要指出的是，随着云计算的深化发展，不同云计算解决方案之间相互渗透融合，同一种产品往往横跨两种以上类型。例如，Amazon Web Services 是以 IaaS 为基础发展的，但新提供的弹性 MapReduce 服务模仿了 Google 的 MapReduce，简单数据库服务 SimpleDB 模仿了 Google 的 Bigtable，这两者属于 PaaS 的范畴；而它新提供的电子商务服务 FPS 和 DevPay 以及网站访问统计服务 Alexa Web 服务，则属于 SaaS 的范畴。

三、大数据技术

（一）大数据的概念

无所不在的移动设备、RFID、无线传感器每分每秒都在产生数据，数以亿计的用户和互联网服务时刻在产生巨大的信息交互。要处理的数据量越来越大，而且还将更加快速地增长，传统的数据处理技术已经无法应付，大数据（Big Data）的出现成为继物联网、云计算之后信息技术领域的又一热点（图 1-6 说明了大数据与云计算的关系）。

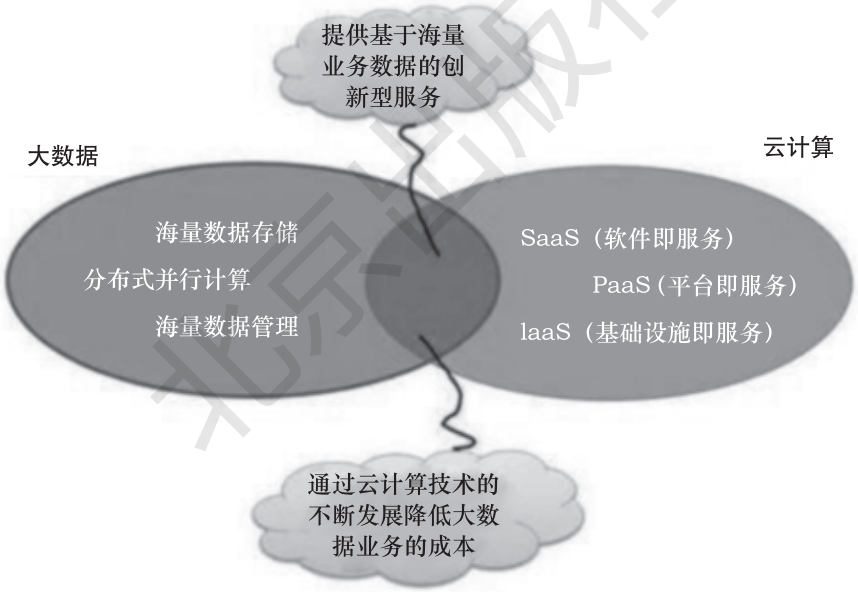

图 1-6　大数据与云计算的关系

大数据由数量巨大、结构复杂、类型众多的数据构成，所设计的信息量规模巨大到无法通过目前的主流软件工具，在合理时间内达到撷取、管理、处理的地步。对数据处理的实施性和有效性提出了更高要求。

大数据无时无刻不在影响和改变着人们的生活。客户在电商网站上有过浏览商品或购物的经历后，就会发现页面上经常会出现一些类似商品的推送信息，这就是电商网站为每个消费者量身定制的商品推荐。通过海量数据能够从客户浏览商品或消费记录里判断出最为精准的商品信息并及时推送给客户，进而促进网站交易额的增长。

（二）大数据的特点

大数据具有以下四个特点，即四个“V”。

1. 数据量（Volume）巨大

大型数据及数据存储量从 TB（1TB=1 024 GB）级别跃升到 PB（1PB=1 024 TB）级别。

2. 数据类别（Variety）繁多

大数据的数据来自多种数据源，数据种类和格式冲破了以前所限定的结构化数据范畴，包括半结构化和非结构化数据。

3. 价值（Value）密度低

以视频为例，在连续不间断的监控过程中，可能有用的数据仅仅为一两秒钟。

4. 处理速度（Velocity）快

处理速度快也是大数据的鲜明特征，其包含大量在线或实时数据分析处理的需求，时效性要求严苛。一般要在秒级时间范围内给出分析结果，时间太长就失去价值了（被称为一秒定律或秒级定律）。

（三）大数据的应用

大数据的应用是利用大数据分析的结果为用户提供辅助决策，发掘潜在价值的过程。大数据的类型大致可分为以下三类：①传统企业数据（Traditional Enterprise Data），包括 CRM Systems 的消费者数据、传统的 ERP 数据、库存数据以及账目数据等。②机器和传感器数据（Machine-generated/sensor Data），包括呼叫记录（Call Detail Records）、智能仪表、工业设备传感器、设备日志（通常是 Digital Exhaust）、交易数据等。③社交数据（Social Data），包括用户行为记录、反馈数据等，如 Twitter、Facebook 等社交媒体平台。

大数据的应用表现在以下几个方面。

1. 企业内部大数据的应用

目前，大数据的主要来源和应用都是来自企业内部，商业智能（Business Intelligence，BI）和 OLAP 可以说是大数据应用的前辈。企业内部大数据的应用可以从多个方面提升企业的生产效率和竞争力。

2. 物联网大数据的应用

物联网不仅是大数据的重要来源，还是大数据应用的主要市场。在物联网中，现实世界中的每个物体都可以是数据的生产者和消费者，由于物体种类繁多，物联网的应用也层出不穷。

3. 面向在线社交网络大数据的应用

在线社交网络是一种在信息网络上由社会个体集合及个体之间的连接关系构成的社会性结构。在线社交网络大数据主要来自即时消息、在线社交、微博和共享空间四类应用。由于在线社交网络大数据代表了人的各类活动，因此，对此类数据的分析得

到了更多关注。在线社交网络大数据分析是从网络结构、群体互动和信息传播三个维度，通过基于数学、信息学、社会学、管理学等多个学科的融合理论和方法，为理解人类社会中存在的各种关系提供的一种可计算的分析方法。目前，在线社交网络大数据的应用包括网络舆情分析、网络情报搜集与分析、社会化营销、政府决策支持、在线教育等。

4. 医疗健康大数据的应用

医疗健康数据是持续、高增长的复杂数据，蕴含的信息价值也丰富多样，对其进行有效的存储、处理、查询和分析，可以开发出其潜在价值。对于医疗健康大数据的应用，将会深远地影响人类的健康。

5. 群智感知

随着技术的发展，智能手机和平板电脑等移动设备集成了越来越多的传感器，计算和感知能力也越发强大。在移动设备被广泛使用的背景下，群智感知开始成为移动计算领域的应用热点。大量用户使用移动智能设备作为基本节点，通过蓝牙、无线网络和移动互联网等方式进行协作，分发感知任务，收集、利用感知数据，最终完成大规模的、复杂的社会感知任务。群智感知对参与者的要求很低，用户并不需要相关的专业知识或技能，只需拥有一台移动智能设备。

6. 智能电网

智能电网是指将现代信息技术融入传统能源网络构成新的电网，通过用户的用电习惯等信息，优化电能的生产、供给和消耗，是大数据在电力系统上的应用。

四、3D 打印技术

（一）3D 打印的概念

3D 打印（3D Printing）是一种新的打印技术，是快速成形技术的一种。它是一种以数字模型文件为基础，运用粉末状金属或塑料等可黏合材料，通过逐层打印的方式来构造物体的技术。

传统的工业制造常采用“减材制造”的方式，即使用机床、夹具和刀具对原材料毛坯进行切、削等减少材料的加工，最终“剩下”要制造的物体。而 3D 打印技术则属于增材制造技术，它直接根据要构造的物体的三维模型数据，通过成型设备以材料累加的方式制成实物。

通过结合工业数字化和自动化等技术，3D 打印技术相对于传统制造技术呈现出三个明显的技术优势：较高的制造自由度、数字化作业流程和较高的原料利用率。当然，3D 打印技术本身也存在很多不足，如批量生产能力弱、设备和材料成本偏高等。3D 打印技术相对于传统制造技术的优势和劣势，如表 1−2 所示。

表 1-2　3D 打印技术相对于传统制造技术的优势和劣势

优势	劣势
复杂部件的加工速度提高，成本降低	简单结构部件的制造速度较慢
功能性产品设计性能提高	直接制造部件的大小受限
产品设计环节速度加快	制造精度相对较低
一体化设计减少组装环节	表面加工质量相对粗糙
制造工具简化	控制软件智能化水平有待提高
能源节约程度提高	使用材料范围和性能相对局限
降低多产品共线的生产成本	设备、材料成本较高

（二）3D 打印原理

3D 打印技术是以计算机三维设计模型为蓝本的。3D 打印时，先通过计算机辅助设计（CAD）完成打印对象的三维模型设计，并用软件将其离散分解成若干层数字切片，然后将这些切片的信息传送到数控成型系统（各类 3D 打印机），利用激光束、热熔喷嘴等方式将粉末状、液状或丝状金属、陶瓷、塑料等材料进行逐层堆积黏结，最终叠加成型，制造出实体产品。

3D 打印技术与普通打印机工作的原理基本相同，用“打印”来通俗地称呼它，也是因为它参照了普通打印机的技术原理。在 3D 打印中，每一个数字切片的加工过程与喷墨打印十分相似，只不过喷墨打印机使用的是纸张和墨水，打印的是二维图像，而 3D 打印中使用的“墨水”是各种实实在在的原材料，最终将若干分层堆叠成三维的实物。

目前，3D 打印的具体实现技术种类繁多，各种技术的区别主要体现为使用的打印材料质地不同、材料形态不同、材料“叠层”的方式不同。目前应用比较多的技术如下。

（1）使用热塑性塑料、共晶系统金属、可食用材料进行挤压的熔融沉积式（FDM）技术。

（2）使用合金线材的电子束自由成型制造（EBF）技术。

（3）使用合金、金属、陶瓷、热塑性塑料等材质颗粒的直接金属激光烧结（DMLS）、电子束熔化成型（EBM）、选择性激光熔化成型（SLM）、选择性热烧结（SHS）、选择性激光烧结（SLS）等技术。

（4）使用石膏粉末的石膏 3D 打印（PP）技术。

（5）使用纸、金属膜、塑料薄膜层压的分层实体制造（LOM）技术。

（6）使用光硬化树脂进行光聚合的液态树脂固化（SLA）和数字光处理（DLP）技术。

（三）3D 打印工作过程

1. 构建三维数字模型并切片

3D 打印的第一个步骤是构建要打印实物的三维数字模型，这是一个 X、Y、Z 三轴的立体模型，是没有分层的结构。一种方法是利用计算机辅助设计（CAD）软件或计算机动画建模软件进行三维设计，构建三维数字模型。另一种方法是利用三维扫描设备对实物对象进行三维测量，将测量数据在计算机中构建为三维数字模型。三维数字模型被保存为一个 STL（标准三角语言）格式文件。STL 格式是设计软件和 3D 打印机之间协作的标准文件格式，能被所有快速成型设备接收，是由 3D Systems 公司发明的。接着，设计软件选定一个 Z 轴的方向，对建成的三维数字模型进行切片（Slice），只有切片之后的模型，才能被 3D 打印机接收并进行逐层打印。这些切片被存为一系列横截面文件。

2. 3D 打印机进行叠层打印

横截面文件传输到 3D 打印机后，就开始了分层加工、叠层成型的 3D 实体打印，在这一基本原理下，不同的 3D 打印技术，使用的打印材料、每一层的加工方式和各层的堆叠方式会有所不同。以最早实用化的 3D 打印技术 SLA（液态树脂固化或光固化，查克·赫尔 1986 年获得专利权）为例，它以光敏树脂的聚合反应为基础。首先在 3D 打印机的工作台上敷一层液态光敏树脂。然后 3D 打印机按照接收到的切片信息，控制激光或紫外光束对光敏树脂进行逐点扫描，使被扫描的树脂薄层（约 0.1 mm）产生聚合反应，由点逐渐形成线，最终形成零件的一个薄层的固化截面，而未被扫描到的树脂保持原来的液态。当一层固化完毕，工作台下移一个层厚的距离，在上一层已经固化的树脂表面再覆盖一层新的液态光敏树脂，用以进行再一次的扫描固化。新固化的一层牢固地黏合在前一层上，如此循环往复，直到整个实体模型制造完毕。

3. 完成实体模型

对于一些结构较简单、精度要求不高的打印对象来说，3D 打印机制造出的实体模型就是成品了。但很多时候由于打印精度和打印工艺的原因，还要经过相应的后续处理，才能完成实体模型产品。3D 打印机的分辨率对大多数应用来说已经足够，但在弯曲的表面可能会比较粗糙。要获得更高分辨率的物品，则可以先用当前的三维打印机打出稍大一点的物体，再对表面进行打磨，得到表面光滑的“高分辨率”物品。有的技术在打印完成后要去除多余的打印材料，比如吹除掉松散的粉末材料，将模型“刨”出来，并把剩余粉末循环利用。有的技术在打印过程中会用到支撑材料，它与打印材料同时使用，对那些镂空、倒挂等结构的物体起支撑作用。这些支撑材料也需要在打印完成后剔除或溶解掉。另外，有时还需要对实体模型进行组装和上色等处理，才能制成最终的产品。

（四）3D 打印机

3D 打印机是 3D 打印的核心装备，是集机械、控制及计算机技术等为一体的复杂

机电一体化系统，主要由高精度机械系统、数控系统、喷射系统和成型环境等子系统组成。

3D 打印机能够实现 600 dpi 的分辨率，每层厚度只有 0.1 mm 甚至更薄，即使模型表面有文字或图片也能够清晰打印。由于打印精度高，打印出的模型除了可以展现出外形曲线上的设计外，结构以及运动部件也可以完全展现。如果用来打印机械装配图，齿轮、轴承、拉杆等都可以正常活动，而腔体、沟槽等形态特征位置准确，甚至可以满足装配要求，打印出的实体还可以通过打磨、钻孔、电镀等方式进一步加工。

针对市场不同，3D 打印机大致可以分为民用级（个人级）和工业级（专业级、生产级）两类，两个级别的 3D 打印机的简单对比，如表 1-3 所示。

表 1-3　3D 打印机的简单对比

类型	民用级 3D 打印机	工业级 3D 打印机
色彩	只能打印单色物体，同一台打印机不能更换耗材	可以直接打印混合彩色物体
价格	几千～几万元不等	十几万～上百万元不等
材料范围	尼龙、塑料、树脂等少数可塑性材料	金属、陶瓷、塑料等常见材料，食品材料、细胞组织等特殊材料
打印速度	手掌大模型需打印几十分钟～几个小时（根据模型复杂程度）	可高速批量打印
打印机体积	普通桌面可放置	体积较大
操作难度	操作简单，需三维设计人员操作	操作复杂，需培训专业人员操作

（五）3D 打印技术应用

3D 打印在全社会的渗透应用需要依托多个学科领域的尖端技术，至少包括信息技术、精密机械和材料科学三大技术。近年来，3D 打印技术发展迅速，在各个环节都取得了长足进步，目前已经在航空航天、制造业、军工、科研、教育、医疗、建筑、艺术、文化等诸多领域得到了一定程度的应用，图 1-7 就是 3D 打印技术的应用成果。

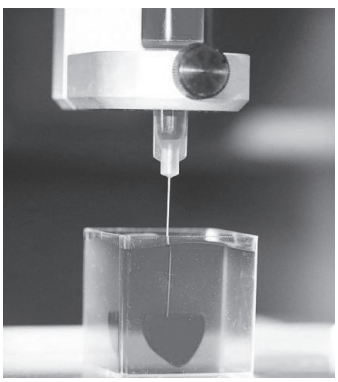

图 1-7　3D 打印技术的应用成果

（1）工业制造方面：产品概念设计，制作模具原型或直接打印模具，产品功能验证，直接打印产品。

（2）航天军工方面：复杂形状、尺寸微细、特殊性能的零部件、机构的直接制造。

（3）生物医疗方面：假牙、假肢、助听器的制造，骨骼、血管、肾脏、肝脏、心脏等可移植的人体组织、器官的制造。

（4）科学研究方面：生物化石扫描 3D 打印和古生物模型复原，纳米材料研究，生物微观结构研究等。

（5）教育领域方面：各种教学和实验模型的制造，对科学假设的验证，对科学现象的直观展示等。

（6）建筑工程方面：建筑实体模型制作，模型风洞实验，建筑工程施工模拟，建筑效果和城市规划的展示等。

（7）食品产业方面：使用各种食材打印人工食品，个性化食品的生产。

（8）文化娱乐方面：各种艺术品和创意文化产品的设计与制作，影视艺术中的道具制作，特效模型制作，动漫角色创作等。

五、人工智能

人工智能，也称机器智能，它是计算机科学、控制论、信息论、神经生理学、心理学、语言学等多种学科互相渗透发展起来的一门综合性学科。人工智能的研究及应用领域包括问题求解、逻辑推理与定理证明、自然语言理解、自动程序设计、专家系统、机器学习、人工神经网络、机器人学、模式识别、机器视觉、智能控制、智能检索和智能调度与指挥等。自人工智能出现以来，科学家们在这些领域的研究已经取得了非常惊人的成果，同时，人工智能使人类超越了自身的局限，人工智能基于大数据分析得到各种新知识、新信息，使人们难以预测的洪水、地震等灾害的预报的精确度大大提高，使人类在自然的约束面前变得更强大，从而更新人们解决问题的方法，拓宽人们解决问题的思路。人工智能的发展已对人类及其未来产生深远影响，本小节将简要介绍人工智能的基础知识。

（一）人工智能的概念

像许多新兴学科一样，人工智能至今尚无统一的定义，要给人工智能下个准确的定义是困难的。人类的自然智能（人类智能）伴随着人类活动时时处处存在。人类的许多活动，如下棋、竞技、解题、猜谜语、进行讨论、编制计划和编写计算机程序，甚至驾驶汽车和骑自行车等，都需要“智能”。如果机器能够执行这种任务，就可以认为机器已具有某种性质的“人工智能”。不同科学或学科背景的学者对人工智能有不同的理解，提出了不同的观点。

关于人工智能，历史上提出了四种定义，代表了四个研究方向。理查德·贝尔曼（Richard Bellman）在 1978 年称智能系统可完成“与人类思维相关的活动，诸如决策、问题求解、学习等”，主张智能机器是像人一样思考的系统。帕特里克·予利·温斯

顿（Patrick Henry Winston）定义智能为理性思考的系统，智能研究即“使知觉、推理和行动成为可能的计算的研究”。伊莱恩·瑞驰（Elaine Rich）和凯文·奈特（Kevin Knight）给出类似图灵测试的定义，称智能为“研究如何让计算机做到那些人比计算机做得更好的事情”。戴维·普尔（David Poole）等则认为“计算智能是对智能化智能体的研究”，主张设计理性行动的系统。

这些定义存在两个差异：第一个差异在于人工智能侧重思维还是侧重行为；第二个差异则是关于智能应该尽可能接近人，还是在一个可知范围内严格地正确或理性思考行事。类人派的研究者借鉴了许多生物学的研究结论和观点，并辅以诸多假设和实验验证。而理性派的研究者则更加侧重通过数学建模解决问题。从人工智能的发展史看，四个研究方向上都有许多人做出了卓越的贡献。这些成果存在互斥的方面，却也有相辅相成的方面，形成了曲折而精彩的历史。

（二）人工智能的发展

人工智能的故事从1956年正式展开。普林斯顿大学的约翰·麦卡锡（John McCarthy）召集全美国对自动机理论、神经元网络和智能研究有兴趣的学者在达特茅斯召开了第一次人工智能研讨会。在达特茅斯会议上，麦卡锡正式提出了人工智能的概念并被沿用至今。1962年，当时就职于IBM的阿瑟·萨缪尔（Arthur Samuel）在IBM7090晶体管计算机（内存仅为32KB）上研制出了西洋跳棋程序，并击败了当时全美最强的西洋棋选手之一罗伯特·尼雷（Robert Nealey），引起了轰动。萨缪尔在研制西洋跳棋程序的过程中，第一次提出机器学习的概念。这些程序能够通过学习达到跳棋业余高手级别，有力地驳斥了计算机只能够执行人给予的命令这种观点。同一时期，艾伦·纽厄尔（Allen Newell）和希尔伯特·西蒙（Herbert Simon）设计的“通用问题求解器”问世，将计算机模型与认知科学的结论结合，证明了伯特兰·罗素（Bertrand Russell）所著《数学原理》中的大多数定理。麦卡锡在1958年搬到麻省理工学院后做出了一系列杰出贡献，包括定义高级语言Lisp，并在发表的论文中描述了使用知识求解问题的一个假想程序（Advice Taker）。该程序可以接受新的公理，并在未重写的情况下获得新的能力，在一定程度上可以实现知识表示和推理。麦卡锡的合作者马文·李·明斯基（Marvin Lee Minsky）更加注重程序如何自动开始运转，选择研究只有智能才可以解决的受限问题，如高等数学中的封闭性积分问题和智力测试中的几何类推问题等。

在研究初期，人工智能爱好者拥有十足的自信和满满的期望，但是这种豪情壮志很快就消失了。首先遇到的一类障碍源于人工智能面向的问题求解困难。大多数早期人工智能程序求解问题的方式是进行组合直至找到解，这种逻辑求解模式在面向较少的行动和较短的解序列时可以奏效，但是在涉及多条定理时，早期的算法就失败了。其次，早期程序缺乏相关主题知识的表达和支撑，导致诸如机器翻译等应用领域遭遇瓶颈。此外，早期关于神经网络的研究也由于成果不佳，科研经费几乎缩减为0。20世纪60年代关于人工智能的里程碑式的事件大致只有两件：第一，1969年，第一

届国际人工智能联合会议（International Joint Conference on Artificial Intelligence，简称为 IJCAI）召开；第二，1970 年，《人工智能》国际杂志（Artificial Intelligence）创刊。

20 世纪 70 年代，人工智能的发展是一个逡巡前进的过程。研究者开发出称为弱方法的通用搜索求解机制，即将基本推理步骤串联起来以寻找完全的解，如在棋局中搜索解空间。专家系统，或称强方法在这个时期也得到关注和探索。

第一个成功的知识型专家系统是爱德华·费根鲍姆（Edward Feigenbaum）等开发的 DENDRAL 系统，由计算机科学家和生物学家合作而成。在 DENDRAL 系统输入分子式和分子的质谱仪信息，可以产生所有符合分子式的可能结构，辅以化学家已知的某些结构的质谱尖峰模式，最后输出分子的最可能形态。DENDRAL 的成功不但验证了费根鲍姆关于知识工程的理论的正确性，而且是人工智能研究的一个历史性突破。

1982 年出现了第一个成功的商用专家系统 R1。这个系统为 McDermott 自动配置订单并且成功节省了数千万美元的成本。这个系统的成功应用激发了美国许多知名公司开始投资开发人工智能专家系统。日本也启动了一项为期 10 年的制造智能计算机的计划。为了与日本抗衡，美国和英国也在国家层面开启了相关研究计划。人工智能工业在 1980—1988 年期间得到的经费迅猛增加。但是研究计划中提及的目标多数并未实现，业界公司也开始承受当初的过分承诺带来的失败。

1986 年后是连接主义的回归时期。这段时间有一个短暂的神经网络研究热潮。神经网络概念源于物理学、心理学和神经生理学的跨学科研究成果。早在 1943 年，第一个神经元数学模型就已经被提出，该模型对神经元的输入信号进行加权，并与阈值进行比较，再决定神经元是否输出。该模型证明了简单的神经元组成网络可以计算所有的数学和逻辑函数。1958 年，心理学家弗兰克·罗森布拉特（Frank Rosenblatt）提出了第一个应用神经网络，即感知机，开启了在模式识别领域的神经网络应用。20 世纪 60 年代，巴纳德·威德罗（Bernard Widrow）等人介绍了类感知机神经网络的学习训练算法。其思想是，网络系统有固定形式的输入和针对输入期望得到的输出值，对期望输出和实际输出之间的误差进行计算以后，使用梯度下降法进行权值调整，从而达到最小均方误差。这已基本奠定了现代的神经网络训练思路。但是，由于当时计算机硬件条件存在极大局限，并且网络构造训练过程需要存储的数据量较大，神经网络的研究暂时被搁置。1980 年以后，随着硬件条件改善，神经网络研究进入了新一轮高潮。由于学界对单层神经网络的性能提出了质疑，复杂多层网络被提出，以解决单层网络无法分类异或问题的缺陷。到了 1980 年，杰弗里·辛顿（Geoffrey Hinton）等人在《自然》杂志上发表的文章系统整理了反向传播算法思想，并为算法冠名反向传播算法，目前使用反向传播算法训练的多层感知机已成为应用最广的神经网络模型。

20 世纪 90 年代起，最风生水起的流派是基于概率统计的建模学习。乌尔夫·格伦德（Ulf Grenander）从 20 世纪 60 年代开始发展随机过程和概率模型。朱迪亚·珀尔（Judea Pearl）于 20 世纪 80 年代提出贝叶斯网络，把概率知识应用于认知推理，并估计推理的不确定性。到 20 世纪 90 年代末，他进一步研究因果推理。2011 年，他因

为对概率统计的人工智能应用做出极大贡献，获得图灵奖。莱斯里·瓦利安特（Leslie Valiant）开创了学习理论，系统而完整地回答了统计学习方法需要多少数据才能以某种置信度习得一种概念。他提出将弱分类器组成强分类器的思想，这推动了一系列集成学习方法的诞生。以Adaboost为代表的Boosting算法，在21世纪初的计算机视觉应用中，可以说达到了深度学习时代前最好的效果。

统计学习中应用最广的算法当属支持向量机算法。支持向量机是一种分类模型。弗拉基米尔·万普尼克（Vladimir Vapnik）在1963年首次提出了支持向量的概念，将支持向量定义为对分类起决定性作用的样本。1995年，弗拉基米尔·万普尼克等人系统总结支持向量方法，提出统计学习理论。支持向量方法在小样本训练集上体现出极佳的性能，并且由于其理论系统成熟，工具包可靠易用，成为学术论文乃至业界应用中常用的基准算法。

随着电视和互联网的普及，大众传媒逐渐将人工智能技术带入了大众视野。1997年，IBM研发的“深蓝”成为第一个击败人类象棋冠军的电脑程序。人工智能开始在全球范围内引起讨论。2006年，杰弗里·辛顿发表“Learning Multiple Layersof Representation”一文，不同于以往学习一个分类器的目标，提出希望学习生成模型的观点。2007年，李飞飞和普林斯顿大学的同事开始建立ImageNet。这是一个大型注释图像数据库，旨在帮助视觉对象识别软件进行研究。有了理论支撑、数据集支持，加上硬件条件较20世纪有了巨大飞跃，神经网络应用开始引爆。多层神经网络，或称深度学习，成为计算机视觉领域表现最好的模型。多层神经网络由于架构灵活、变种多样，也成功适应诸如自然语言处理、推荐系统等丰富的应用场景，带来焕然一新的效果。

（三）人工智能的分类

分类学与科学学研究科学技术学科的分类问题，本是十分严谨的学问，但对于一些新学科却很难确切地对其进行分类或归类。例如，多数学者至今仍把人工智能看作计算机科学的一个分支，但从科学长远发展的角度看，人工智能可能要归类于智能科学的一个分支。智能系统也尚无统一的分类方法，按其作用原理可分为下列几种系统。

1. 专家系统

专家系统（Expert System，ES）是人工智能和智能系统应用研究最活跃和最广泛的领域之一。自从1965年第一个专家系统DENDRAL在美国斯坦福大学问世以来，经过20年的研究开发，到20世纪80年代中期，各种专家系统已遍布各个专业领域，取得很大的成功。现在，专家系统得到更为广泛的应用，并在应用开发中得到进一步发展。

专家系统是把专家系统技术和方法，尤其是工程控制论的反馈机制有机结合而建立的。专家系统已广泛应用于故障诊断、工业设计和过程控制。专家系统一般由知识库、推理机、控制规则集和算法等组成。专家系统所研究的问题一般具有不确定性，是以模仿人类智能为基础的。

2. 模糊系统

扎德（L. Zadeh）于1965年提出的模糊集合理论成为处理现实世界各类物体的方法，

意味着模糊逻辑技术的诞生。此后，对模糊集合和模糊控制的理论研究与实际应用获得广泛开展。1965—1975 年，扎德对许多重要概念进行了研究，包括模糊多级决策、模糊近似关系、模糊约束和语言学界限等。此后 10 年，许多数学结构借助模糊集合实现模糊化。这些数学结构涉及逻辑、关系、函数、图形、分类、语法、语言、算法和程序等。

模糊系统是一类应用模糊集合理论的智能系统。模糊系统的价值可从两个方面来考虑。一方面，模糊系统提出一种新的机制用于实现基于知识（规则）甚至语义描述的表示、推理和操作规律。另一方面，模糊系统为非线性系统提出一个比较容易的设计方法，尤其是当系统含有不确定性而且很难用常规非线性理论处理时，更是有效。模糊系统已经获得十分广泛的应用。

3. 神经网络系统

人工神经网络（Artificial Neural Networks，ANN）研究的先锋麦卡洛克（McCulloch）和皮茨（Pitts）曾于 1943 年提出一种叫作“似脑机器”（Mindlike Machine）的思想，这种机器可由基于生物神经元特性的互连模型来制造，这就是神经学网络的概念。到了 20 世纪 70 年代，格罗斯伯格（Grossberg）和科霍恩（Kohonen）以生物学和心理学证据为基础，提出了几种具有新颖特性的非线性动态系统结构和自组织映射模型。沃博斯（Werbos）在 20 世纪 70 年代开发了一种反向传播算法。霍普菲尔德在神经元交互作用的基础上引入一种递归型神经网络（霍普菲尔德网络）。在 20 世纪 80 年代中叶，作为一种前馈神经网络的学习算法，帕克（Parker）和鲁姆尔哈特（Rumelhart）等重新发现了反向传播算法。近十年来，深度学习网络得到深入研究和广泛应用。AlphaGo 国际围棋程序的核心就是深度学习。现在神经网络已在从家用电器到工业对象的广泛领域找到其用武之地，主要应用涉及模式识别、图像处理、自动控制、机器人、信号处理、管理、商业、医疗和军事等领域。

4. 学习系统

学习（Learning）是一个非常普遍的术语，人和计算机都通过学习获取知识，改善技术和技巧。具有不同背景的人们对学习具有不同的看法和定义。

学习是人类的主要智能之一，在人类的进化过程中，学习起到了很大作用。

进入 21 世纪以来，人类对机器学习的研究取得新的进展，尤其是一些新的学习方法为学习系统注入了新鲜血液，必将推动学习系统研究的进一步开展。

5. 仿生系统

科学家和工程师们应用数学和科学来模仿自然，包括人类和生物的自然智能。人类智能已激励出高级计算、学习方法和技术。仿生智能系统就是模仿与模拟人类和生物行为的智能系统，人类试图通过人工方法模仿人类智能已有很长的历史了。

生物通过个体间的选择、交叉、变异来适应大自然环境。生物种群的生存过程普遍遵循达尔文的物竞天择、适者生存的进化准则。种群中的个体根据对环境的适应能力而被大自然所选择或淘汰。进化过程的结果反映在个体结构上，其染色体包含若

干基因，相应的表现型和基因型的联系体现了个体的外部特性与内部机理间的逻辑关系。把进化计算（Evolutionary Computation），特别是遗传算法（Genetic Algorithm，GA）机制用于人工系统和过程，则可实现一种新的智能系统，即仿生智能系统（Bionic Intelligent Systems）。

6. 群智能系统

我们可以把群（Swarm）定义为某种交互作用的组织或真体（Agent）的结构集合。在群智能计算研究中，群的个体组织包括蚂蚁、白蚁、蜜蜂、黄蜂、鱼群和鸟群等。在这些群体中，个体在结构上是很简单的，而它们的集体行为却可能变得相当复杂。社会组织的全局群行为是由群内个体行为以非线性方式实现的。于是，在个体行为和全局群行为间存在某个紧密的联系。这些个体的集体行为构成和支配了群行为。另一方面，群行为又决定了个体执行其作用的条件。这些作用可能改变环境，因而也可能改变这些个体自身的行为和它的地位。

群社会网络结构形成该群存在的一个集合，它提供了个体间交换经验知识的通信通道。群社会网络结构的一个惊人的结果是它们在建立最佳蚁巢结构、分配劳力和收集食物等方面的组织能力。群计算建模已获得许多成功的应用，从不同的群研究得到不同的应用。

7. 多真体系统

计算机技术、人工智能、网络技术的出现与发展，突破了集中式系统的局限性，并行计算和分布式处理等技术（包括分布式人工智能）及多真体系统（Multiple Agent System，MAS）应运而生。我们可以把真体（Agent）看作能够通过传感器感知其环境，并借助执行器作用于该环境的任何事物。当采用多真体系统进行操作时，其操作原理随着真体结构的不同而有所差异，难以给出一个通用的或统一的多真体系统结构。

多真体系统具有分布式系统的许多特性，如交互性、社会性、协作性、适应性和分布性等。多真体系统包括移动（Migration）分布式系统、分布式智能、计算机网络、通信、移动模型和计算、编程语言、安全性、容错和管理等关键技术。

多真体系统已获得十分广泛的应用，涉及机器人协调、远程控制、远程通信、柔性制造、网络通信、网络管理、交通控制、电子商务、数据库、远程教育和远程医疗等。

8. 混合智能系统

前面介绍的几种智能系统，各自具有固有优点和缺点。例如，模糊逻辑擅长处理不确定性，神经网络主要用于学习，进化计算是优化的高手。在真实世界中，不仅需要不同的知识，还需要不同的智能技术。这种需求导致了混合智能系统的出现，单一智能机制往往无法满足一些复杂、未知或动态系统的系统要求，这就需要开发某些混合的（或称为集成的、综合的、复合的）智能技术和方法，以满足现实问题提出的要求。

混合智能系统在相当长的一段时间成为智能系统研究与发展的一种趋势，各种混合智能方案如雨后春笋一样纷纷面世。混合能否成功，不但取决于结合前各方的固有特性和结合后“取长补短”或“优势互补”的效果，而且也需要经受实际应用的检验。

此外，还可以按照应用领域来对智能系统进行分类，如智能机器人系统、智能决策系统、智能加工系统、智能控制系统、智能规划系统、智能交通系统、智能管理系统、智能家电系统等。

（四）人工智能的应用领域

人工智能的研究领域包括自然语言处理、自动定理证明、自动程序设计、智能检索、智能调度、机器学习、机器人学、专家系统、智能控制、模式识别、视觉系统、神经网络、Agent、计算智能、问题求解、人工生命、人工智能方法和程序设计语言等。在过去的 60 年中，已经建立了一些具有人工智能的计算机系统，如能够求解微分方程的，下棋的，设计分析集成电路的，合成人类自然语言的，检索情报的，诊断疾病以及控制太空飞行器、地面移动机器人和水下机器人的具有不同程度人工智能的计算机系统。

六、区块链

2015 年以来，区块链技术引起了学术界和产业界的高度关注，被认为是继大型机、个人电脑、互联网、移动社交网络之后计算范式的第五次颠覆式创新，很可能带来新一轮技术革新和产业变革。区块链是一种新技术，虽然目前其应用还未普及，但已成为近年来最火的信息技术之一。下面简单介绍区块链的诞生、区块链技术、区块链分类及其商业价值。

（一）区块链的诞生

1. 区块链的概念

关于区块链的定义，有很多说法，目前尚未形成一个被普遍接受的定义。工业和信息化部指导发布的《中国区块链技术和应用发展白皮书（2016）》中，这样定义区块链：“广义来讲，区块链技术是利用块链式数据结构来验证与存储数据、利用分布式节点共识算法来生成和更新数据、利用密码学的方式保证数据传输和访问的安全、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的一种全新的分布式基础架构与计算范式。”这个定义对于大众而言可能过于技术化，区块链不仅仅是一种技术架构和计算范式，更是一种理念，而这种理念很容易被大众理解和应用，并且将被融入生活的各方面。

从技术层面看，区块链是一种只支持增加、查询的去中心化分布式数据库系统。与传统的中心化数据库不同，区块链系统由多个分布式去中心化节点构成，每个节点既充当客户端也充当服务器端，节点与节点之间可以自由连接，用户之间可以实现信息的传输和服务，无须中心环节和服务器的介入。

举个通俗易懂的例子，在一座城市中，市民统一维护着一份关于本市所有交易的账本。一天，张三借给李四一万元，并向全市广播通知。其他市民得到通知并确认了这笔交易，将该笔交易记录在自己的账本中，形成统一的公认化账本，即公共账本。几天后，李四突然耍赖，宣布自己没有向张三借过钱。此时，其他市民通过查询自己的账本，确认了李四确实向张三借过一万元，且后续没有还款记录，所以可证明李四

在撒谎。

从上面的例子中可发现，这座城市已建立了一个交易系统，交易过程不需要第三方机构作信用背书。城市中每个人的权利和义务都是平等的，共同维护同一份账本，所有数据公开、透明、完整且难以篡改。所以，区块链技术解决了信用共识的问题。

蜂群给了我们很好的示范。蜂群思维是一种集体思维。任何一只蜜蜂的智慧都是有限的，但当这些独立的蜜蜂高度连接时，可形成一个高智慧的活系统。蜂群的智慧远远超出所有个体智慧的总和。

构建去中心化的互联网生态，可能会帮助解决传统中心化网络所遇到的各种问题。去中心化的网络中接入的个体越多，系统将更加强大、安全和公平。

2. 区块链的历史渊源及与比特币的关系

区块链是由一系列技术实现的全新经济组织模式，2009 年诞生于比特币系统的构建过程中，2017 年成为全球经济热点，但目前区块链的成功应用寥寥，这个新兴产业还远未成熟。为方便理解区块链的历史与趋势，下面将介绍区块链的历史渊源及其与比特币的关系。

若要探寻区块链的机制和发展，还要从 1982 年莱斯利·兰伯特（Leslie Lamport）提出的拜占庭将军问题说起。拜占庭是东罗马帝国的首都，位于如今的土耳其的伊斯坦布尔。拜占庭拥有大量财富，邻邦垂涎已久。由于当时东罗马帝国地域宽广，守卫军队之间相隔甚远，军队的将军们只能通过信使传递消息。在战时，军队的所有将军和副官必须对攻打哪支敌军达成一致决定。但由于军中可能存在叛徒，他们错误的信息传递会干扰将军们的决定，影响一致性的达成。如何在此种情况下，让忠诚的将军不受叛徒的影响，达成行动的一致，就是所谓的拜占庭将军问题。

早先针对拜占庭将军问题的传统解决方案有口头协议算法、书面协议算法等，但这两种方法都存在一些明显的缺陷。口头协议算法的消息无法溯源，书面协议算法虽然解决了口头协议算法的不足，却没有考虑个体之间信息传输的时延、实现困难以及依赖中心化的数据记录与管理。所以在很长一段时间，拜占庭问题始终找不到一个完美的解决方法。然而解决区块链问题并不等同于解决拜占庭将军问题，目前区块链系统的大多共识机制旨在解决拜占庭将军问题，却很难突破效率瓶颈。

2008 年 10 月，一个化名为中本聪的团队提出比特币的概念并发布了《比特币：一种点对点的电子现金系统》一文。2009 年，第一批 50 个比特币在一台小型服务器上被挖出。

伴随着比特币的发展，越来越多的问题暴露出来。面对比特币本身受到的种种质疑以及热潮的退却，人们逐渐将目光从比特币转向其底层支撑技术——区块链。

至此，可能有些人会产生疑问：区块链不就是比特币吗？其实这是一种误解，区块链因比特币而生，由于比特币是区块链的第一个应用，且在早期远比其底层区块链技术更受欢迎，人们才将二者混淆。其实中本聪并没有提及“区块链”这一概念，但其发布的比特币开源代码实现了去中心化的记账功能，且公开、透明、难以篡改，而

这些代码就是区块链技术的雏形。

近期，区块链得到了更多的关注和更快的发展，继而引发了分布式应用热潮。目前，针对区块链进行底层设施开发的项目逐渐增多，但要形成切实可用的成果还有很长的路要走，区块链作用的真正实现需要面向异构信息处理、面向应用，具备高可靠性、高效率的底层系统。

（二）区块链技术

区块链虽然是一个新概念，却不是一种单一、全新的技术，它由多个现有技术优化组合而成，包括点对点（P2P）网络技术、分布式账本技术（Distributed Ledger Technology，DLT）、共识机制、密码学、数据库技术、社会网络、经济学等。这些技术单独来看相对成熟，但通过巧妙的组合后形成了一种新的、特殊的去中心化分布式数据库系统。下文将对组成区块链的几个主要技术进行简要介绍。

1. P2P 网络技术

P2P 网络是一种计算机网络的组成方式，与传统的中心化服务器加客户端结构不同，它是分散的、去中心化的。在 P2P 网络中，各个节点不再区分服务器端和客户端的关系，所有节点的地位平等，不存在中心化的控制机制。相比中心化的网络结构，P2P 网络拥有更好的并行处理能力、扩展性以及强大性。图 1-8 展示了中心化网络与 P2P 网络的结构差异。

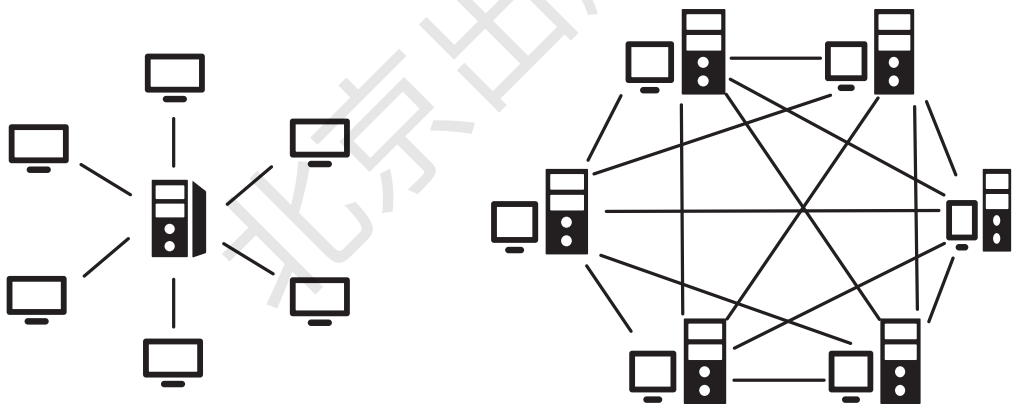

图 1-8　中心化网络与 P2P 网络的结构差异

区块链系统不依赖任何第三方的控制来保障整个系统的运行，这与 P2P 网络的特点高度契合。另外，P2P 网络技术是发展成熟的计算机技术，已被广泛用于开发各种分布式应用。因此，区块链采用 P2P 网络协议，以实现去中心化控制。

区块链是一个对等的动态网络，网络中时刻有新节点的加入和旧节点的退出。当系统中新增节点数目大于退出节点数目时，整个系统的容量也将扩大。

2. 分布式账本技术

分布式账本本质上是一种由多个节点、不同物理地址或者多个成员共同维护的账目数据，以实现数据的分享、同步和复制的去中心化数据库。分布式账本技术推翻了

传统的记账模式，网络中的参与者都有一份真实账本的完整备份，账本中可以存储多种类型的资产。

账本中账目数据的更新或修改会在所有节点的副本中反映出来，任何人想私自篡改账本数据必须改动大部分节点存储的账本，这加大了篡改账本的难度。

区块链技术实质上是一种采用了加密算法（如哈希算法）的分布式账本技术。哈希算法是区块链中保证交易信息难以被篡改的单向密码机制，它通过接收一段明文，并以一种不可逆的方式将明文压缩映射成为一串长度固定的随机散列输出。

区块链中的其他节点通过简单的哈希计算即可验证该区块链的哈希值是否正确、信息是否被篡改。区块链的分布式账本结构如图 1-9 所示。

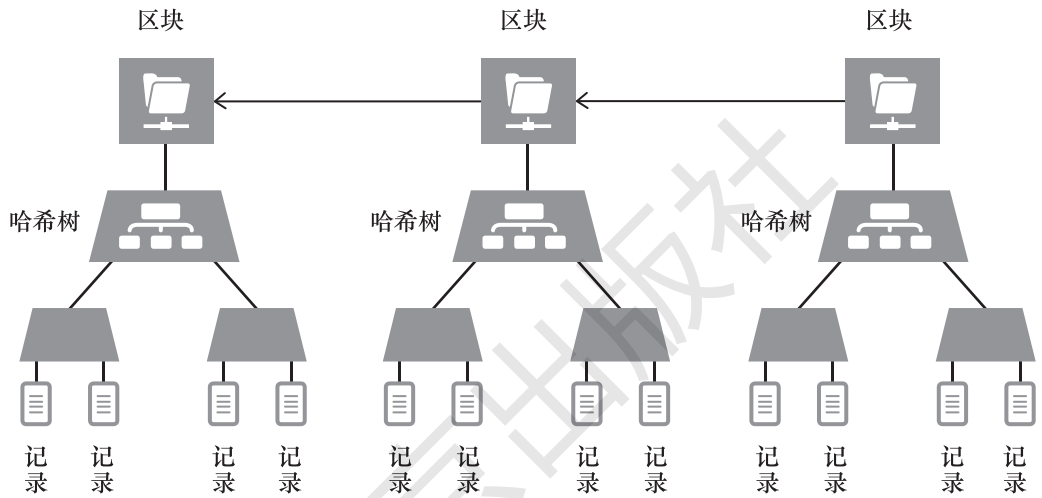

图 1-9　区块链的分布式账本结构

3. 共识机制

区块链之所以能成为一个难以攻破的、公开的、难以篡改数据记录的去中心化系统，原因有以下两点：一是选择一个随机的节点产生一个区块；二是使分布式数据记录不可逆。这两个方面的技术核心就是共识机制。共识机制是区块链节点就区块信息达成的全网一致认可的机制，可以保证最新区块被准确添加至区块链、节点存储的区块链信息一致不分叉甚至可以抵御恶意攻击。当前主流的共识机制包括工作量证明（Proof of Work，PoW）、权益证明（Proof of Stake，PoS）、股份授权证明（Delegated Proof of Stake，DPoS）等。

工作量证明是这样一种机制：拥有算力越多的节点，其单位时间内付出的工作量越大，利用其算力寻找运算问题所需的时间越短，因而相应地获得记账权的概率也越高。某些节点充当矿工消耗自身算力进行特定的运算来找到符合一定要求的哈希随机数，其中最快的矿工获取当前区块的记账权，并获得奖励。工作量证明的优缺点如表 1-4 所示。

表 1-4　工作量证明的优缺点

优点	缺点
算法简单，容易实现	算力要求高，能源浪费大
节点间无须交换额外的信息	区块的确认时间长，效率低
恶意攻击花销巨大	可能但不易产生硬分叉

权益证明是这样一种机制：节点获得记账权的概率与所持有数字资产的数量及时间成反比，这类似于现实生活中的股东机制。节点通过提供一定量的保证金来证明合法的交易块，恶意的节点的保证金则将被没收。权益证明的优缺点如表 1-5 所示。

表 1-5　权益证明的优缺点

优点	缺点
恶意攻击需要足够的数字资产	仅经济壁垒设计较计算资源容易突破
挖矿不再需要消耗大量的能源	容易产生超级节点
缩短了达成共识时间，性能提升	容易产生分叉

股份授权证明是这样一种机制，区块链的正常运转依赖于受托人（Delegates），受托人的数量由项目方决定，一般为 100 个。受托人的对象则由每个持币用户投票决定，每个用户的投票权重与其持币量成正比。项目的受托人完全等价，受托人的节点服务器充当矿机，负责打包区块、维持系统的运转且能获得相应的奖励。股份授权证明的优缺点如表 1-6 所示。

表 1-6　股份授权证明的优缺点

优点	缺点
资源消耗少、吞吐量高	投票率不高
共识相对快	容易造成安全隐患

除上述机制外，还有瑞波共识协议（Ripple Consensus Protocol，RCP）、恒星共识协议（Stellar Consensus Protocol，SCP）、DAG 算法协议（Directed Acyclic Graph）、Pool 验证池机制、实用拜占庭容错机制（Practical Byzantine Fault Tolerance，PBFT）和 PoL 位置证明协议（Proof of Location）等，这些机制中有些甚至已经应用在区块链系统中，不同共识机制各有其应用场景和优势。

4. 密码学

密码学的历史可追溯到古埃及时期，至今已有数千年的历史。密码学早期主要应用在军事和外交领域，而后随着科技的发展逐渐进入公众领域。信息是社会发展的重要资源，信息技术的发展推动了传统产业的改造和经济的增长，而信息安全则是信息技术发展的前提。

如果要在数据世界中保障信息安全，那么必须用到密码学，区块链也不例外。在区块链技术中，使用多种密码学技术将数据和区块以时间顺序相连，形成一种难以篡改、难以伪造的链式数据结构。这些技术包括：哈希算法、加密算法、数字签名、梅克尔树（Merkle Trees）等。其中，哈希算法技术保障了区块链的完整性；加密算法技术保障了区块链的机密性；数字签名技术保障了数字内容的完整性和不可抵赖性；梅克尔树减少了确认完整性所付出的代价。此外，还有一些现代密码学技术被应用到区块链中，这些技术的结合利用保障了区块链的长期健康发展。

（三）区块链分类及其商业价值

区块链系统根据应用场景和用户需求的不同，技术应用的类型一般分为公有链、联盟链和私有链（表 1-7）。除此之外，目前也存在多链结构，支持多个公有链，多层次或者嵌套的链结构。

表 1-7　三种类型区块链的对比情况

	公有链	联盟链	私有链
参与者	任何人	组织成员	企业内部成员
管理者	所有参与人	组织协商规定	自定义
共识机制	PoW/PoS	投票 / 多方共识	投票 / 多方共识
中心化程度	去中心化	部分去中心化	中心化
交易速度	慢	快	快
用户量	数百万	数万	数百

1. 公有链

公有链是指任何人都可以在任何时候加入或退出、任意读取数据以及参与交易和记账的区块链。公有链通常也称为非许可链，它做到了真正意义上的完全去中心化。公有链通过利用密码学技术保障去中心化环境下交易的安全性和难以篡改性。

公有链的应用场景非常广泛，如互联网金融等。这些公有链项目使用的共识机制一般是工作量证明、权益证明等。

2. 私有链

私有链是指其读写权限由私有组织或企业机构制定的区块链。一般而言，私有链的写入权限控制在私有组织手中，如公司或企业，而读取权限则由组织制定，组织可对不同的群体或个人进行不同程度的读取限制。

有人认为私有链跟传统的中心化的数据库没有区别，甚至处理效率也不及中心化数据库，因此觉得私有链没有存在的必要。事实上，中心化和去中心化永远是相对的，如果将私人组织或机构看成一个整体，私有链则可看成运行在该整体内的公有链。此外，私有链也具有一般区块链的价值，包括安全、可溯源、难以篡改以及智能合约，这些价值都是传统数据库系统难以提供的。与公有链相比，私有链还有另外一大优势，那就是处理速度相对较快，主要是因为私有链网络中节点少，且大多数情况下无须挖

矿来验证交易，所以交易速度较公有链有了很大的提升。

3. 联盟链

联盟链是指由若干个组织或机构共同参与维护的区块链，其内部指定多个节点共同记录交易数据，其他节点可以参与交易但没有记账权。联盟链介于公有链和私有链之间，可实现部分去中心化，并且可控性强、交易速度快。联盟链一般用于银行、保险、证券、商业协会、集团企业及上下游企业。

信息安全与病毒防范