目录 CONTENTS

第一章

区块链技术基础理论

第一节　区块链基本概念

一、区块链的定义

作为一种新兴信息技术，区块链在最近几年引起广泛关注。去中心化架构、分布式共识、智能合约，各种新技术名词不断涌现，区块链溯源、区块链发票、区块链保险、区块链司法，各种区块链应用层出不穷。这些专业化的技术名词和多样化的应用场景让区块链技术越发带有神秘感。到底什么是区块链？区块链为什么能够得到各方的关注？区块链技术从哪里来，又将如何改变未来的生活场景？这些问题都是了解区块链的敲门砖。

在给出正式的定义之前，我们用日常生活中一个常见的例子来介绍为什么需要区块链技术。此例子来源于新华社 2019 年针对区块链技术的一篇文章，贴近生活实际，能够生动的展示区块链技术的特点。比如，现在患者如果需要去多个医院治疗，经常会遇到数据不同步、重复做检查的困扰。这种现象不但消耗了患者的大量精力与财力，更是对医疗资源的极大浪费。之所以出现这样的情况，是由于各家医院采用了相互独立的信息系统，对于患者自行携带的检查资料，医生无法确认数据真实性。那么能否建立跨越多家医院的分布式医疗数据库？把患者在不同医院的就医数据全部保存在一个分布式数据库中，每个医院都保存一份完整的信息备份。这样，患者在任意一家医院就医，都不用进行重复检测。对于上述分布式数据库功能，传统的基于中心架构的信息系统将面临多种难题。包括：不同医院之间如何保证数据一致性问题，如何解决数据篡改、伪造问题，如何保护用户隐私和各个医院的核心利益，如何在出现医疗纠纷时解决多方矛盾，等等。

区块链技术正是为了解决多个机构之间数据共享、协同工作的难题而产生。在此应用中，通过构建由多个医院共同维护的区块链网络，能够保证各方公平地参与数据维护和

系统运行的操作，避免单方以及少数恶意用户进行数据篡改、数据伪造攻击。

在此案例中，患者信息打包组成的数据单元，被称为区块。每个区块之间采用密码技术从逻辑上链接到一起，串成一条数据链，就是我们说的区块链。通过这种区块链的方式管理患者数据，不但能方便患者在不同医院间进行就诊，还具有很多特殊的优势，第一是数据更加安全，区块链模式中，所有医院同时保存了大量冗余的数据备份。即使一家医院的数据库发生意外，患者的信息依然是安全的，能够有效应对数据丢失、数据篡改、系统宕机等单点故障。数据更加可信。区块链中采用严格证明的密码技术保证数据不可篡改、不可伪造。患者数据一旦上传，很难对其进行篡改，患者也无法抵赖自己的数据，保证系统中的医疗数据具有更高的可信度。第二是数据隐私得到有效保护，患者的检测信息十分敏感，数据共享过程中可能泄露用户的隐私，利用区块链技术能够实现可授权的数据共享，保证患者数据只能由授权的医生在授权模式下使用，避免原始数据直接共享导致的隐私泄露隐患。正是由于区块链具备的这些独特优势，使得区块链技术能够从一种数字货币应用中脱颖而出，被应用到众多行业。

关于区块链是什么？这是个很复杂的话题，区块链源自比特币，也是比特币的一个重要概念，是比特币的底层技术。其实，区块链技术并不是一种单一的、全新的技术，而是多种现有技术（如加密算法、P2P 文件传输等）整合的结果，这些技术与数据库巧妙地组合在一起，形成了一种新的数据记录、传递、存储与呈现的方式。不同的人有不同的职业背景和知识结构，从不同的角度，不同的出发点，对区块链会有不同的理解和解读。简单来说，区块链是分布式数据存储、点对点传输、共识机制、加密算法等计算机技术的新型应用模式。

“区块链”起源于一篇由化名为“中本聪”（Satoshi Nakamoto）的学者在 2008 年发表的奠基性论文《比特币：一种点对点电子现金系统》，论文提出区块链技术被用于实现一种不依赖中间人的点对点电子货币系统。由于论文中使用了“chain of blocks”这个词组来介绍系统底层结构，我国研究人员在翻译这个句子的时候，就直接用了“区块链”一词，而后这个词就直接被写成了“blockchain”，成为代表区块链技术体系的专有名词。

狭义的区块链技术是一种按照时间顺序将数据区块以链条的方式组合成特定数据结构，并以密码学方式保证的不可篡改和不可伪造的去中心化共享总账，能够安全存储有先后关系的、能在系统内验证的数据。广义的区块链技术则是利用加密技术来验证与存储数据，利用分布式共识算法来新增和更新数据，利用运行在区块链上的代码，即智能合约，来保证业务逻辑的自动强制执行的一种全新的多中心化基础架构与分布式计算范式。

2016 年 10 月，我国工业和信息化部原信息化和软件服务业司指导发布的《中国区块

链技术和应用发展白皮书》将区块链描述为分布式数据存储、点对点传输、共识机制、加密算法等计算机技术在互联网时代的创新应用模式。

狭义来讲，区块链是一种按照时间顺序将数据区块以顺序相连的方式组合成的一种链式数据结构，并以密码学方式保证其成为不可篡改和不可伪造的分布式共享账本。通俗地说，区块链就是指一种全民参与记账的方式。区块链系统中，每个人都可以有机会参与记账。在一定时间段内如果有任何数据变化，系统中每个人都可以来进行记账，系统会评判这段时间内记账最快最好的人，将他记录的内容写入账本，并把这段时间内的账本内容发给系统内所有人进行备份。这样系统中的每个人都有了一本完整的账本。

从数据的角度来看，区块链是一种分布式数据库，这里的“分布式”不仅体现为数据的分布式存储，也体现为数据的分布式记录（即由系统参与者来集体维护）。简单地说，区块链能实现全球数据信息的分布式记录（可以由系统参与者集体记录，而非由一个中心化的机构集中记录）与分布式存储（可以存储在所有参与记录数据的节点中，而非集中存储于一个中心化的机构节点中）。我们过去和现在的数据库，不管是阿里巴巴、腾讯，还是工商银行，通常是采用中心化的数据库。所有的系统里都会有一个数据库，我们可以把数据库看成是一个大账本。目前情况是谁的系统就由谁来记账，比如微信的账本就是由腾讯在记，淘宝的账本就是由阿里巴巴在记，工商银行的账本就是由工商银行在记。

同时，区块链实现并建立了分布式信用体系，是现有互联网的升级，转变为从信息传递升级到价值传递。也就是说，我们过去的互联网和现在的互联网，实现的是信息的传输，而将来的区块链网络，不仅仅是传递信息，更能实现价值的传输和信用的传输。

在我国，区块链作为一个全新的概念和理论正在发展之中，虽然在行业领域如阿里巴巴、百度、腾讯、中国联通、平安科技、工商银行等已经布局区块链并且部分已经取得世界领先的成绩和地位，但是大众（甚至一些 IT 和互联网从业人员）对其认知、研究和实践的程度基本上都是才刚刚起步。要想在这一领域弯道超车，引领世界，还需要理论研究者、网络技术者、金融从业者，以及政府监管部门的积极投入和良性互动。

二、区块链的分类

（一）根据应用范围

1. 公有链

公有区块链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，也是目前应用最广泛的区块链。各大 bitcoins 系列的虚拟数字货币均基于公有区块链，世界上有且仅有一条该币种对应的区块链。公有区块链的安全由“加密数字经济”维护，“加密数字经济”采取工作量证明机制或权益证明机制等共识方式，将经济奖励和加密数字验证结合起来，并遵循着一般原则。

公有链的任何节点都是开放的，每个人都可以参与这个区块链中的计算，而且链上的任一节点都可以共享所有数据，即全部账本。公有链一般通过发行代币（Token）来鼓励参与者竞争记账（即挖矿），确保数据的共识性和安全更新。

2. 联盟链

联盟区块链也有时称为联合区块链或者行业区块链。联盟区块链的节点地位并不均等，记账节点一般由某个群体内部指定或者预选而来，每个块的生成由所有的预选节点共同决定。普通接入节点权限很小，可以参与交易，但无权参与记账过程。也就是说，预选节点参与共识过程，其他节点本质上还是托管记账，联盟链虽然也是分布式记账，但并不像公有链那样“人人平等”，公众仅可以通过该区块链开放的 API 进行限定查询。

联盟链参与者追求公平和透明的协作模式，主要用于实现节点间的可信数据交换。联盟链的各个节点通常有与之对应的实体机构组织，通过授权后才能加入或退出网络。联盟链的数据只允许系统内不同的机构进行读写和交易，而且不同的节点可能有不同的权限。

3. 私有链

私有区块链，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；读取权限或者对外开放，或者被任意程度地对其进行了限制。私有链并没有实现分布式记账或存储，不具有区块链去中心化的属性，所以业内也有很多人并不认为私有链是区块链。

在某些区块链的应用场景下，开发者并不希望任何人都可以参与这个系统，因此建立一种不对外公开，只有被许可的节点才可以参与并且查看所有数据的私有区块链。私有链一般适用于特定机构的内部数据管理与审计。

4. 公有链与私有链详解

业内也有人认为联盟链介于公有链和私有链之间，但实质上仍属于私有链的范畴。目前金融机构多偏向联盟链，但这也可能只是暂时过渡的状态。联盟链可视为“部分去中心化”的区块链，公众可以交易和查询，但无记账权限，如发布智能合约需获得联盟许可。

世界上早期的区块链都是公有链，公有链是完全开放的区块链，全世界的人都可以参与系统的维护工作。私有链或联盟链在开放程度和去中心化程度方面有所限制，不同的节点可以被赋予不同的权限，而且权限高低可能是悬殊的，并不像公有链那样一切讲究平等和透明。

（1）公有链。

公有链是任何节点都能参与其中共识过程的区块链——共识过程决定哪个区块可被添加到区块链中并明确当前状态。公有链通常被认为是“完全去中心化”的。公有链的具有极低地访问门槛的特点，只要一台接入网络的计算机就可以访问公有链，每个公有链一般都会推出一些工具软件，用户安装软件后便可以快速便捷的访问公有链。并且所有数据默认公开，一般所有关联的参与者都会隐藏自己的真实身份，这在公有链中是非常普遍存在的。典型的公有链如比特币网络就是完全透明公开的，每一个人都能通过比特币区块浏览器（Bitcoin Block Explorer）看到历史上以及正在发生的每一笔交易。还可以保护用户免受开发者的影响在公有链中程序开发者无权干涉用户，比如比特币网络的发明人也无法干涉或控制比特币用户。

公有链包括比特币、以太坊、莱特币和几乎所有山寨币，其中公有链的始祖是比特币区块链。以“以太坊”为例来说明，以太坊是一个全新开放的区块链平台，它允许任何人在平台中建立和使用通过区块链技术运行的去中心化应用。与比特币相同的地方是：以太坊不受任何人控制，也不归任何人所有。与比特币不同的地方是：以太坊是可编程的区块链，更像是一台台分布式计算机，允许用户按照自己的意愿创建复杂的操作。以太坊也可被理解为分布式操作系统，以太币仅仅是其中的一小部分。以太坊支持多种语言编程，所以其具有无限的应用可能，就像我们手机上的各类应用软件，通过编程构建出包罗万象的世界。以太坊尤其适合那些点与点之间进行直接自动交互或多节点协调活动的应用。除金融类应用外，任何对信任、安全和持久性要求较高的应用场景——如资产注册、投票、管理和物联网等都会大规模地受到以太坊平台的影响。

（2）私有链。

私有链是指其写入权限仅在一个组织手里的区块链。读取权限或者对外开放会被任意程度地限制。

私有链的特点是交易速度非常快，一个私有链的交易速度可以比任何其他的区块链都要快，甚至接近了常规数据库的速度（常规数据库即传统数据库，是相对于区块链的分布式数据库而言的），因为私有链记账和确认只需要在少数节点上进行，相对于公有链的共识确认需要众多节点而言，极大地提升了效率。并且隐私保障更好，因为私有链只有少

数已经授权的节点会拥有完整的权限，这些节点可能就是主管领导或者单位，其余节点和面向公众的查询访问会被严格设定。这便可以胜任隐私保护要求更高的场景。还可以将交易成本大幅降低甚至为零，私有链的交易只需要几个权限高的节点确认即可，其交易成本与公有链相比极低。在虚拟数字货币交易所，比特币的转账手续费通常是0.2%，这个费用包含了交易所的利润，实际上每笔比特币交易确实是需要支付给矿工手续费的，比如价值5美元的比特币交易与价值5000美元的比特币交易需要支付给矿工的手续费可能是相同的。同时还有助于保护其基本的产品不被破坏，私有链与传统金融机构的管理和运营模式非常类似，更加容易被相关行业人士接受，这也保证了传统金融机构可以继续拥有既有产品的稳定。如此就不难理解为什么银行和政府对私有链或联盟链可以做到欣然接受。

Linux基金会在2015年12月主导发起的超级账本项目（Hyperledger project）是一个旨在推动区块链跨行业应用的开源项目，成员包括金融、物联网、供应链、制造和科技行业的领头羊。R3CEV是一家总部位于纽约的区块链创业公司，由其发起的R3区块链联盟，已吸引了50家巨头银行的参与，其中包括富国银行、美国银行、纽约梅隆银行、花旗银行等，中国平安银行于2020年5月加入R3区块链联盟。2016年4月，R3联盟推出了Corda项目，这是一个专门为银行业准备的分布式金融解决方案。Corda是一个区块链平台，可以用来管理和同步各个组织机构之间的协议。

有的专家认为私有链（联盟链）可以有效地解决传统金融机构的效率、安全和欺诈问题，也能给许多金融企业提供公有链无法解决的解决方案。私有链（联盟链）确保入网者遵守规章制度，比如医疗保险可携性和责任法案（HIPAA）、反洗钱（AML）和客户身份验证（KYC）制度。其实，公有链、私有链、联盟链都是区块链技术的一个细分，而技术仅仅是一种工具，如何在不同的场景应用好不同的工具才是技术进步的关键所在。

（二）根据部署机制

1. 主链和主网

通常区块链都有主网和测试网。主网是区块链社区公认的可信区块链网络，其交易信息被全体成员所认可。有效的区块在经过区块链网络的共识后会被追加到主网的区块账本中。主链是主网节点共同维护的区块链。

2. 测试链和测试网

测试网是对应主网的具有相似功能但主要用于测试的网络。由于测试链是为了在不破坏主链的情况下尝试新想法而建立的，只用于测试，因此测试链上的测试币在主网中不

具备交易价值。比如，比特币的测试链已经多次重置，以阻止将其测试币用于交易、投机的行为。

（三）根据对接类型

1. 侧链

侧链是主链外的另一个区块链，链接锚定主链中的某一个节点，通过主链上的计算力来维护侧链的真实性，实现公有链上的数据或数字资产与其他账簿上的数据或数字资产在多个区块链间的转移。最具代表性的实现有 Blockstream，这种主链和侧链协同的区块链架构中的主链有时也被称为母链（Parentchain）。

比特币主要是按其设计者中本聪的思想设计的一个虚拟货币系统，虽然很成功，但是其规则已经相对固定，很难在比特币上做大的修改，因为这些修改会引起分叉，影响现有的比特币用户。因此，要在比特币平台上做创新或扩展是比较困难的。一般来说，大部分代币系统是通过用比特币平台做基础，重构一条区块链，然后在上面使用新的规则发新的虚拟货币。这就是目前大部分代币的做法。然而这些代币系统要从无到有得到人们的价值认可是非常困难的，通常的办法是与比特币挂钩，相当于用比特币作为储备来发行代币，这样就可以完成代币的货币价值认可的过程。但随之而来的问题是如何自动保障代币和比特币的挂钩，因为虚拟货币的一个特点就是价格波动非常大，一般人都不愿意持有波动大、流动性差的代币。一个直接的想法就是通过比特币平台和代币平台的整合来做到实时的挂钩。

2. 互联链

针对特定领域的应用可能会形成各自垂直领域的区块链，互联链就是一种通过跨链技术连接不同区块链的基础设施，包括数据结构和通信协议。各种不同的区块链通过互联链互联互通并形成更大的区块链生态。与互联网一样，互联链的建立将形成区块链的全球网络。

三、区块链的特征

区块链是比特币的底层技术，像一个分散的数据库账本，记载所有的交易记录。区块链是一种分布在类似于 NoSQL（非关系型数据库）这样的技术解决方案的统称，并不是某种特定技术，它能够通过很多编程语言和架构来实现。实现区块链的方式很多，仅从共

识机制角度来讲，包括工作量证明机制、权益证明机制、股份授权证明机制等。再回到比特币来说区块链，我们不要把比特币当成一种货币，而是要当成一个总账，它是一个电子总账，网络上每个参与者的电脑都有一份总账的备份，并且所有的备份都会实时的持续的对账同步。

从信息系统架构层面来看，区块链本质上承担了数据存储的作用，类似一个特殊的数据库。例如，溯源应用中，区块链的主要作用是存储物流数据。但是，不同于普通的数据库，区块链技术有许多独特的技术特征。在架构层面，区块链系统采用去中心化网络架构；在数据层面，区块链具有数据防篡改的突出优势；在运行层面，区块链采用多方协作的运行模式；在应用层面，区块链技术能够构建去中介的信任体系。

区块链的“区块”是一串使用密码学方法相关联产生的数据块，每一个数据块中包含了一次比特币网络交易的信息，用于验证其信息的有效性和生成下一个区块。区块链的特征，行业内并没有完全统一的说法，但就整体来说，区块链主要具有以下特征。

（一）去中心化

去中心化网络架构是指区块链系统建立在没有中心节点的分布式网络之上。不同于微信、支付宝等常见的应用系统，区块链系统中不存在一个独立的中心服务器管理和维护所有的交易数据，而是由分布式节点协作完成交易数据的转发和运维工作。这种去中心化的网络架构使区块链网络具备了高冗余的通信链路，能够有效抵抗单点崩溃问题，提高针对网络攻击的防御能力。

由于使用分布式核算和存储，不存在中心化的硬件或管理机构，任意节点的权利和义务都是均等的，少数节点即使停止工作都不影响系统整体的运作，系统中的数据块由整个系统中具有维护功能的节点来共同维护。通过对比来看，日常生活中的银行结算或支付系统等，需要一个中心服务器或中心机构才能完成。而比特币的结算系统是分散地建立在网络上的，它会是一个去中心化的结算数据库方式。

（二）开放性

区块链系统是开放的，除了交易各方的私有信息被加密外，区块链的数据会对所有人公开，任何人都可以通过公开的接口查询区块链数据和开发相关应用，因此整个系统信息高度透明。

区块链系统各个层次的运行过程都是建立在多方协作的基础上，包括底层代码升级、

系统日常运维、分歧处理调节等。区块链系统中任何重要事宜都不能由任何一方独立决定，而是必须依靠多方协作，在共识机制等协议的调控下达到多数用户的认可。通过采取集体决策原则解决系统运行面临的各项问题，区块链系统具有较强的公信力和适应能力。

（三）自治性

区块链的自治性体现在多参与方、多中心的系统按照基于协商一致的规范和协议来自动运行，最终确保记录在区块链上的每一笔交易的准确性和真实性。运行的过程完全按照符合规范的触发条件执行，任何人为干预不起作用。比如区块链的强安全、共识机制不需要第三方的进入，而是通过一个先前预定的技术来实现整个交易的完成。

由于节点之间的交换遵循固定的算法，其数据交互是无须信任的（区块链中的程序规则会自行判断活动是否有效），因此交易双方无须通过公开身份的方式让对方对自己产生信任。比特币就具有强匿名性，所以到现在也找不到真正的中本聪（比特币的发明人）。

（四）安全性、稳定性和可靠性

系统中每一个节点都拥有最新的完整数据库拷贝，一旦信息经过验证并添加至区块链，就会永久的存储起来。除非能够同时控制系统中超过 51% 的节点，否则单个节点上对数据库的修改是无效的。系统会自动比较，认为最多次出现的相同数据记录为真。同时，它是一个分布式的网络架构，没有一个中心节点可以被打击或者攻击，所以在整体的技术布置方面有着更强的安全性、稳定性、可靠性和持续性，以及信息永久不可篡改。

为了解决去中心架构下分布式节点的数据一致性问题，区块链中利用了多重技术确保数据不可篡改。首先，采用散列函数等密码技术对所有数据进行完整性验证，能够高效地检测数据是否被篡改；采用时间戳技术对每个时间段的数据进行打包封装，确保每一份链上数据都具有明确的时间属性，增加篡改的难度；采用激励机制鼓励所有节点参与账本维护过程，利用大量节点产生的合力来抵御少部分用户的恶意攻击。上述多种技术的协同合作确保了区块链账本中的数据具备不可篡改和不可伪造的优良特性。

（五）去信任

区块链网络内，所有节点能够在去信任的环境下自由安全的交换数据。“去信任”这个词在区块链领域会经常出现，“去信任”就是在整个系统中的多个参与方无须互相信任

就能够完成各种类型的交易和协作。去信任，去的是人的信任，区块链使得对人的信任改成了对机器的信任。

区块链系统的核心价值在于提供一种去中介的信任体系，即非可信节点之间，可以在无须第三方中介的条件下实现可信交易。区块链建立的去信任体系是对传统基于中介信任体系的重大创新，能够减少中介成本、提升交互效率。

第二节　区块链技术原理

一、区块链技术设计

（一）网络信任

1. 数据更可信

传统网络中，数据通常被强势参与方以中心化方式存储，业务数据难以共享。数据可信度由数据持有者以商业信用保证，只能建立主观信任。当社会监督机制失灵，其他参与者需要付出额外的成本来降低数据被恶意篡改的风险。区块链将数据输入历史按时间先后顺序链在一起，并通过共识机制使得参与各方共同验证和拥有这些数据。由于众多节点全部持有相同的数据副本，在密码技术下保证了数据几乎不能被篡改，因此降低了信任风险，使得数据更可信。

2. 契约履行更可信

传统合约由于是事后依人的主观意愿执行，合约履行成效受参与主体个体主观因素影响极大，只要其中一方违约，另一方就需要付出高昂的成本（担保、保险、律师费、漫长的司法程序等）才能完成追索，有时甚至得不偿失。而区块链的智能合约却不一样，只要触发条件满足，计算机程序就会自动执行智能合约，参与主体之间的数字化资产账户数据就会按合约规定完成转移，由此，履约成本被大为降低、交易确定性提高。契约可信是社会人际往来的基础，区块链智能合约重建了契约自动实现机制，必然会给社会带来深远的积极影响。

3. 长周期交易效果更能达到预期

传统业务在多主体开展时，往往因很难判断间接主体提供信息的真实性、有效性而增加风险；并且，还会因业务的隔离，而致使主体间难以延伸出多级或跨级业务。区块链技术通过保证了长周期交易链条中各参与主体的身份真实、数据可信，以及实现价值与信用的多级传递，从而免去中介背书等因缺乏信任导致的摩擦成本，促进业务扁平化发展，提升多方交易效率，使长周期交易效果更能达到预期。

4. 交易历史完整、可追溯

当交易产生时，区块链会将交易及其时间戳全部记录下来，为参与交易的各方保留可信的历史记录，并提供对历史的追溯查询，从而基本保证了交易的不可篡改和不可抵赖。

（二）非对称加密

区块链共识过程中，以大规模汇聚众多共识节点的算力资源，来实现共享区块链账本的数据验证和记账工作，类似于一种共识节点的任务众包过程。在区块链去中心化系统中的共识节点，其本身具有自利性，其最大化自身收益是参与数据验证和记账的根本目标。因此，区块链系统通过设计适度的经济激励机制是一种相容的合理的众包机制，使得共识节点因最大化自身收益的个体行为与保障区块链系统的安全有效的整体目标相符合，而形成了对区块链历史的稳定共识。

在密码学史上，非对称加密的出现是一个重要的里程碑。其使用的公钥概念解决了对称加密的单密码方式中最难解决的密钥分配问题和数字签名问题。在非对称加密体系中，密钥被分解为公钥和私钥一对，公开密钥用于加密，私有密钥用于解密。私有密钥只能由生成密钥的交换方掌握，公开密钥可广泛公布，但它只对应于生成密钥的交换方。非对称密钥有两种使用方式，传送保密信息和消息认证。

1. 传送保密信息

通过实现多个用户用公钥加密的消息只能由一个用户用私钥解读，而实现在公共网络中的通信保密。

2. 消息认证

由于公钥是公开的，一个用户用私钥加密的消息可被其他多个用户用对应的公钥解读，因此，可实现认证系统中对消息进行数字签名和证明消息的来源。非对称加密方式因

其使通信双方无需事先交换密钥就可建立安全通信的特点，而广泛应用于身份认证、数字签名等信息交换领域。

（三）保护隐私

1. 区块链网络是一种 P2P 网络

P2P 网络很难实现网络窃听，节点之间采用中继转发的模式进行通信，杜绝了传统网络中通过窃听网络流量发现用户之间通信关系的问题。

2. 区块链技术支持匿名交易

区块链交易中使用的地址通常由用户自行创建和保存，不需要第三方参与，地址本身和用户身份信息无关；此外，区块链地址通常具有非常大的地址空间，出现碰撞的概率非常低，这使得用户可以为每次交易生成不同的地址，从而增强交易的匿名性。

3. 采用区块链技术的应用程序通常是去中心化架构

而去中心化架构能够有效应对网络攻击，不需要在中心服务器上存储账户、密码等敏感信息，从而能够避免传统服务器被攻击而导致的数据泄露风险。

（四）包容性

在全球，大概有 20 亿的成年工作者没有机会享受正规的金融服务。撒哈拉以南非洲地区，只有 24% 的成年人拥有银行账户。那些流入发展中国家的资金，往往在当地产生高额的交易费用，无法真正帮助那些想要创业的居民。在这种情况中，互联网只是集权于某小部分玩家的东西，由此极其不利于创业者。区块链有效地解决了这种问题，其可以助力创新发展的企业精神，并为他们提供更好地获得资本的渠道；其有着巨大的包容性和普惠性，极大地降低了交易成本，比如资金转移和汇款；降低了拥有属于自己银行账户、获取信用和投资的门槛；提高了个人创业和国际贸易的参与度；它不仅仅是资本再分配，更开创了新的资本分配方式。

目前，已有一些团体和机构开始致力于推进和倡导区块链的包容性，并帮助个人和社区接触了解区块链和一些新科技生态系统，为不同的人群提供发展机会。在这些包容性举措中，我们发现，目前在区块链领域，女性数量大体上领先，这一发现和我们之前在互联网时代初期的情况截然相反。繁荣的基础是包容，包容包含了方方面面，它意味着社会

霸权、经济霸权、种族霸权的终结，也意味着康歧视、性别歧视、性别鉴定的终结，而区块链能够为这些人类理想的实现提供支持。通过让技术更人性化，发展包容性，最终消除歧视，连接全球经济和企业实体，这是区块链价值设计的另一贡献。

二、区块链架构原理

现代社会日益复杂，社会治理日渐成为最重要的议题。如何才能实现社会的良性治理有些人说依靠国家法律，也有些人说依靠伦理和道德。这两种说法固然正确。但是，对于治理的对象即活生生的人而言，这种外部规制始终过于表面化，缺少必要的中间环节。换一个角度理解，社会良性治理呈现为人们和谐生活，这种和谐来自人们内心的确信，这个由内而外的确信即为信任，来自交互对象彼此行为效果的可预期。因此，正确的说法应该是，并非规则实现了社会治理，而是人与人之间基于信任实现了社会治理，规则只是在一定程度上提升或者降低该种信任，加固或减损了社会治理的效果。在缺少信任的社会环境中，规则非但难以促使人们良性互动，而且还会成为一种破坏人们良性互动的工具。所以，规则按照这样的逻辑发挥作用：人们预测交互对方也会服从自己所服从的规则，基于这种认识，人们彼此相信对方，和谐生活。规则背后另有规则。所以，埃里克森认为，“是规范，而不是法律规则，才是权利的根本来源”。也就是说，规范是本，而法律规则是表。这里的规范主要是指社会规范，表现为人与人之间的信任规则。

关于信任的作用，许多著作均有所涉及。目前主流观点认为，信任属于社会资本，作为润滑社会交互关系的善意储备，可以增加社会财富，相反，缺乏信任，非但不能提升效率，而且会造成资源的极大浪费。美国学者凯文·韦巴赫最近提出的信任架构（trust architectures）概念，对我们理解信任的产生以及社会治理有很大帮助。在韦巴赫看来，信任是一种架构，具有催生的原点和辐射的范围。他按照这个标准将信任架构区分为三种：利维坦（Leviathan）信任架构、点对点（peer-to-peer）信任架构和无需信任的信任（Trustless Trust）架构。

（一）利维坦信任架构

利维坦信任架构是指以集中机构为原点而形成的信任架构，民众由于信任集中机构而进行社会交互。譬如，我们信任不动产登记机关的权威，进而放心通过其对不动产信息记录来昭示产权。我们信任银行的权威，进而放心通过其对汇兑和支付信息进行记录来表示货币的移转。我们信任法院，进而放心将我们与别人的纠纷交由其进行处理，并遵守其

作出的裁判结果。民众之所以对集中机构有彼此信任，是因为其背后有国家强力支撑，如果违背了该信任架构，违背者会受到惩罚。正是由于该种信任架构的明确性与可预期性，以及赏罚分明措施，其可以辐射至一个国家的地域全境。这种普遍化的信任架构也是目前世界最主流的社会交互治理模式。

利维坦信任架构的典型例子是以股票交易为核心建立起来的资本市场。资本市场的特质决定了政府机构的高度介入。首先，在资本市场中，金融机构主要使用“别人的钱”进行投资，所以，其中的交易基本上属于代理关系，容易诱发机会主义风险。其次，在资本市场中，交易双方都需要知道对方的详尽信息，信息披露成为交易的核心要求。最后，资本市场具有系统性风险，一旦出现问题，一方面会影响国内其他经济领域，另一方面也会影响其他国家的资本市场安全。上述问题不能通过交易者达成联盟而解决，也不能通过法院的事后介入解决，只能通过发挥中央政府的事前监管作用而解决。

由信任集中机构衍生的社会交互存在一些问题：第一，集中机构保管的官方交互记录可能会出错，第二，维持官方交互记录需要花费高昂成本。人们之所以放心去和陌生人交易，是因为一般都相信银行和产权登记机关保管的交互记录不会出错。但是，事实并非如此。除了集中机构职员有意篡改之外，交互记录也会出现其他的错误情形，如果集中机构以自己的方式对记录进行判断，就会产生纠纷。譬如，某个人的银行资产记载余额为1000元，而个人主张其真实账户余额为10000元，双方争执不下。为了得到公正结果，可以去银行内部申诉，但是层级处理是银行管理的要求，需要经过许多层级审批，最后或许可以找到解决纠纷的出口。这将是一个漫长的过程。各种流水单以及存款是否被人提取，需要自动取款机的提取记录等，这一切都需要被证明。如果内部解决不畅，需要第三方介入。譬如，可以诉诸法院，但司法程序更是烦琐无比，即使让职业律师介入，也需要花费很高的时间成本。为了维持交互记录，防止记录灭失，集中机构需要电子备份，为了防止发生电子系统遭受黑客入侵等危险，甚至需要进行纸质备份，并且将其保存在一个极其安全的地方，而这些保存成本会非常高昂。随着网络社会的到来，交互者扩及全球范围而让本国政府鞭长莫及，匿名交互让政府难以追及交互者的真实身份，以政府为主导的信任架构的运行效率降低，社会治理面临严峻挑战，亟待机制创新。

（二）点对点信任架构

点对点信任架构是希望能够消除集中机构消极作用的一种尝试。它是指基于我们对长期互动而产生的人际关系和共同社区规范的信任而产生的信任架构。在该信任架构里，

相互信任的人之间具有共同的交互背景，信守自己群体自创的交往规则，即劳伦斯·莱斯格所说的社会规则（social norms），这种自觉意识在一定程度上消解了集中机构的作用。交互者彼此之间相信对方不会破坏规则，比如在鸡尾酒会上，你偶尔失礼，但相信对方基于涵养不会让自己难堪。我相信你，并非因为有集中机构的存在，而是因为我信任你这个人。基于此，集中机构被排除在信任架构之外，个体的人而非抽象的集中机构成为信任的原点。

点对点信任架构最有名的例子就是中世纪商人们构造起来的交互网络。该网络的目的在于排斥权威机构对于社会交往的介入。关于商人之间交互关系的规范，不再依靠王室制定的法律，而是依靠商人之间心照不宣的某种社会规则，“商人间实行合作，不论采用什么形式，都需要忠诚、信任，以及恪遵指令。由此形成一种相当严格的商业道德”。这也是奥斯特罗姆（Elinor Ostrom）、罗伯特·埃里克森（Robert Ellickson）和其他人发掘到的公共管理（commons regimes）领域，在那里无需法律也可以实现社会秩序。对于当事人之间的交互而言，良好表达的社会规范和标准，加上人们对自身声誉的珍视足矣。后来，商人们将这些规范加以整理，制定成所谓的商人法（Law Merchant）。“商人们自发聚集到一起，制定共同的游戏规则。商业法律由此诞生。它没有得到国家的承认，完全是自发产生，自行裁决并强制实施，就像一个俱乐部的规章制度一样。”商人不仅创制规则，而且建立了执行该规则的机构，“商人组建自己的法庭来执行源于自愿合同交易的自设法律框架”。这种规则虽然是一种软规范，但商人们轻易不敢违反，否则将会被孤立，寸步难行。

基于点对点信任架构建立起来的交互网络也有弱点：第一，不像利维坦信任架构那样，点对点信任架构的辐射范围有限，基于此而构建起来的社会交互网络半径不够广大。因为如果脱离开某种个体或者某种文化背景，特定的信任架构就可能失效。譬如，我国传统社会的宗族信任，超出族群范围的人们之间不会产生信任。地区商会成员可以相互信任，超出该圈子则很难自动产生信任。第二，它依靠经常瞬息变化的社会联系和非正式治理结构。如果人们之间的社会联系降低，则信任架构就会发生变化，或者产生转向。譬如，突然有些人不愿意再信任社区规则，如果范围较小，社区会进行矫正，如果范围逐渐扩大，本应信守规则的人认为继续信守规则会对自己不利，通过理性考虑后，他也可能会选择破坏规则。因此，没有强力支持，难以成就良性的社会治理。

（三）无需信任的信任架构

传统的社会治理的两种模式虽然逻辑有差异，但本质上却相同：都属于人对人的治

理。在利维坦信任架构中，集中机构执行者往往由自然人担当。在点对点架构中，也是将信任原点置于具体的自然人身上。由于是人对人的治理，最后难免受到作为执行者或者被信赖者的人之机会主义行动倾向的影响。区块链的出现，为社会治理提供了第三种信任架构：无需信任的信任架构。即通过一系列技术，催生分布式共识网络。

这种新的范式让信任系统输出成为可能，交互网络的形成并不需要其中的任何行动者。区块链通过技术支撑起来的信任架构可以超越上述两种信任架构，首先，交互者不再依赖于集中机构，信任点不在于中心，而是去中心，表现为分布式节点，而且这些节点通过协商表决的方式实现。其次，交互者也不再信赖相对的行动者，该架构的特点不再停留在对交互对象的信任上，而是超越了对人的信任，因此成为无需信任的信任。最后，该信任架构建立起来的交互网络可以超越上述信任架构建立起来的交互网络。理论上而言，基于区块链的交互网络可以足够广大，达到超乎想象的程度。凡是使用区块链的用户，无论身处何地，身份为何，都会形成交互网络。所以，它的信任范围可以超越国界和某种紧密的共同体。

无需信任的信任架构的典型例子是智能合约。智能合约表现为一段代码，被嵌入区块链中，如果代码预先设定的条件满足，就会自动执行交易者的意图。与传统合约不同的是，代码一旦运行则不得被停止或者修改，这杜绝了交易者的机会主义行为。由于区块链底层协议的精神是“代码即法律”，因此，借助于区块链，智能合约排除了第三方在交易中的自由裁量权，其目的在于打造一个独立的“法外世界”。基于区块链，人们不再信赖权威机构，只要相信带有密码与算法的机器即可。就像莱斯格所言，“重要的规则，不是通过社会制裁，也不是通过国家，而是通过特定空间的架构强加的。一个规则不是通过法规来定义的，而是通过管理空间的代码来定义的”。

有学者提出了较为中肯的观点，“密码学和软件可以取代守门人，但这并不意味着我们完全不相信人类”。无需信任的起点和终点都是人，活生生的自然人。而人之最重要的社会价值即是自由。算法和机器的确可以导致一个高度定制性和确定性秩序的形成，这个秩序可以消除机会主义和各种人力所导致的混乱，从而提升社会效率。但是，这种高度定制性和确定性秩序在一定程度上会消解自由。因为人们借助于区块链作出选择之后，不得偏离代码这一规律，从这个意义上而言，人们之间的交互被其下层的技术代码所自动强制执行，而不再顾及各交互方的意愿。代码即法律不可能容忍错误，即当代码承载的并非交互者的真意，或者距离交互者的真意有差距时，代码依然强制执行，依托于区块链从追求确定性的目标走向不正义的确定性目标。

三、区块链技术难点

（一）技术本身的特性受限

毋庸置疑，区块链技术对于金融业、医疗行业、公证、通信领域等各个领域的发展都将产生不可估量的作用，但是，即便如此，区块链依然存在一些不可避免的技术挑战。根据现在实际情况来看，区块链在各个领域中的应用并没有非常成熟，其原因主要在于区块链本身的交易速度非常慢——这是当前区块链在应用过程中所面临的一个重要的技术挑战。

区块链技术体系非常复杂，它涉及密码学、计算数学、人工智能等诸多跨学科、跨领域的一些前沿学科，一些普通的工程师很难在短期内去完全掌握它。

（二）场景应用受限

当前，区块链的应用场景，主要集中于虚拟货币类场景、记录公证类场景、智能合约场景、证券应用场景以及社会事务场景等，与我们大众生活仍然有相当的距离，让人觉得不够接地气；因此，对于区块链技术的追捧，目前主要集中于一些高中端人群和企业中。以互联网协议为技术的区块链，如果没有一个庞大的用户群作为发展基础的话，在未来的发展前景将会受到极大的限制，将很难突破大众、主流市场。

（三）安全性问题

从互联网角度来讲，任何时候，都不能够轻信一个系统是绝对安全的。区块链也存在着安全性的技术局限。

1. 51% 攻击

区块链需要引入大量公共资源参与到体系中来，若参与计算的节点数太少、则会面临 51% 攻击的可能性，对体系的良好运转产生威胁。另外，攻击者还可以将攻击对象转换为攻击使用的个人，如侵入个人的钱包或者攻击相关平台等，因为用户与钱包之间的别名身份在匿名性上其实是相当弱的，加之区块链交易具有公开、透明的特点，任何人可以通过观察区块链得出关于某事的结论。

2. 私钥与终端安全

在目前比特币的机制下，私钥存储在用户终端本地。如果用户的私钥被窃取，将对

用户资金造成严重损失。区块链如何解决私钥易被窃取的难题，仍需探索。

3. 共识机制安全

现阶段情况下，多种基于区块链的共识机制已被提出，包括 PoW、PoS 等；但这些共识机制能否实现真正的安全，仍缺乏严格的证明与试验；因此，如何保障共识机制的安全是一大挑战。

（四）扩展性问题

区块链本身是一个非常难以预测的系统，不论是其商业模式还是技术创新，当扩展到一定数量级的时候，由谁来承担责任就会成为一个难以解决的问题。数据在区块链上确权的问题实际上是由资源本身的特点所决定的。现实中竞争性资源可以放到区块链上进行交换，而知识产权、非竞争性资源目前还并不适合在区块链上进行交换。

当然，区块链的发展前景是十分光明的，对于各领域发展的促进作用也是不言而喻的，但是要想借助区块链技术快速推进各领域的持续快速发展，所面临的种种技术挑战依然是当前研究的主要方向以及亟待解决的重点。

第三节　区块链技术背景

一、大数据技术

（一）定义与特点

大数据是指无法在一定时间内用常规软件工具对其内容进行抓取、管理和处理的数据集合。大数据技术，是指从各种各样类型的数据中，快速获得有价值信息的能力。适用于大数据的技术，包括大规模并行处理（MPP）数据库，数据挖掘电网，分布式文件系统，分布式数据库，云计算平台，互联网，和可扩展的存储系统。

大数据由巨型数据集组成，这些数据集大小常超出人类在可接受时间下的收集、使用、管理和处理能力。高德纳于 2012 年修改对大数据的定义：“大数据是大量、高速及多变的信息资产，它需要新型的处理方式去促成更强的决策能力、洞察力与最优化处理。”

大数据必须借由计算机对数据进行统计、比对、解析方能得出客观结果。数据挖掘则是在探讨用以解析大数据的方法。具体来说，大数据具有 4 个基本特征，一是数据体量巨大，百度资料表明，其新首页导航每天需要提供的数据超过 1.5PB（1PB=1024TB）。二是数据类型多样，现在的数据类型不仅是文本形式，更多的是图片、视频、音频、地理位置信息等多类型的数据，个性化数据占绝对多数。三是处理速度快，数据处理遵循“1 秒定律”，可从各种类型的数据中快速获得高价值的信息。四是价值密度低。以视频为例，一小时的视频，在不间断的监控过程中，可能有用的数据仅仅只有一两秒。

（二）大数据的应用价值

谈及价值，首先必须要弄清楚其用户到底是谁？有针对企业数据市场的，还有针对终端消费者的，还有针对政府公共服务的；其次要弄清楚大数据核心价值的表现形式、价值的体现过程以及最后呈现的结果。商业的发展天生就依赖于大量的数据分析来做决策，对于企业用户，更关心的还是决策需求，其实早在 BI 时代这就被推上了日程，经过十余年的探索，如今已形成了数据管理、数据可视化等细分领域，来加强对决策者的影响，达到决策支持的效果。还有企业营销需求，从本质上来说，主要聚焦在针对消费者市场的精准营销。对于消费者用户，他们对大数据的需求主要体现在信息能按需搜索，并能提供友好、可信的信息推荐，其次是提供高阶服务，例如智能信息的提供、用户体验更快捷等等。还有，大数据也不断被应用到政府日常管理和为民服务中，并成为推动政府政务公开、完善服务、依法行政的重要力量。从户籍制度改革，到不动产登记制度改革，再到征信体系建设等等都对数据库建设提出了更高的目标要求，而此时的数据库更是以大数据为基础的。可见，大数据已成为政府改革和转型的技术支撑杠杆。数据，除了它第一次被使用时提供的价值以外，那些积累下来的数据海洋并不是无用的废物，它还有着无穷无尽的“剩余价值”，关于这一点，人们已经有了越来越多的认识。事实上，大数据已经开始并将继续影响人们的生活，接下来会探索大数据的核心价值，当然这是需要借助于一些具体的应用模式和场景才能得到集中体现的。

1. 有助于企业挖掘市场机会

随着大数据的发展，企业也越来越重视数据相关的开发和应用，从而获取更多的市场机会。一方面，大数据能够明显提升企业数据的准确性和及时性；另一方面，还能够降低企业的交易摩擦成本；更为关键的是，大数据能够帮助企业分析大量数据而进一步挖掘细分市场的机会，最终能够缩短企业产品研发时间、提升企业在商业模式、产品和服务上

的创新力，大幅提升企业的商业决策水平，降低了企业经营的风险。

大数据能够帮助企业分析大量数据而进一步挖掘市场机会和细分市场，然后对每个群体量体裁衣般的采取独特的行动。获得好的产品概念和创意，关键在于到底如何去搜集消费者相关的信息，如何获得趋势，挖掘出人们头脑中未来会可能消费的产品概念。用创新的方法解构消费者的生活方式，剖析消费者的生活密码，才能让吻合消费者未来生活方式的产品研发不再成为问题，如果了解了消费者的密码，就知道其潜藏在背后的真正需求。大数据分析是发现新客户群体、确定最优供应商、创新产品、理解销售季节性等问题的最好方法。

在数字革命的背景下，对企业营销者的挑战是从如何找到企业产品需求的人到如何找到这些人在不同时间和空间中的需求；从过去以单一或分散的方式去形成和这群人的沟通信息和沟通方式，到现在如何和这群人即时沟通、即时响应、即时解决他们的需求，同时在产品和消费者的买卖关系以外，建立更深层次的伙伴间的互信、双赢和可信赖的关系。

大数据进行高密度分析，能够明显提升企业数据的准确性和及时性；大数据能够帮助企业分析大量数据而进一步挖掘细分市场的机会，最终能够缩短企业产品研发时间、提升企业在商业模式、产品和服务上的创新力，大幅提升企业的商业决策水平。因此，大数据有利于企业发掘和开拓新的市场机会；有利于企业将各种资源合理利用到目标市场；有利于制定精准的经销策略；有利于调整市场的营销策略，大大降低企业经营的风险。

企业利用用户在互联网上的访问行为偏好能为每个用户勾勒出一幅“数字剪影”，为具有相似特征的用户组提供精确服务满足用户需求，甚至为每个客户量身定制。这一变革将大大缩减企业产品与最终用户的沟通成本。例如：一家航空公司对从未乘过飞机的人很感兴趣（细分标准是顾客的体验）。而从未乘过飞机的人又可以细分为害怕飞机的人，对乘飞机无所谓的人以及对乘飞机持肯定态度的人（细分标准是态度）。在持肯定态度的人中，又包括高收入有能力乘飞机的人（细分标准是收入能力）。于是这家航空公司就把力量集中在开拓那些对乘飞机持肯定态度，只是还没有乘过飞机的高收入群体。通过对这些人进行量身定制、精准营销取得了很好的效果。

2. 大数据提高决策能力

当前，企业管理者还是更多依赖个人经验和直觉做决策，而不是基于数据。在信息有限、获取成本高昂，而且没有被数字化的时代，让身居高位的人做决策是情有可原的，但是大数据时代，就必须要让数据说话。

大数据能够有效地帮助各个行业用户做出更为准确的商业决策，从而实现更大的商业价值，它从诞生开始就是站在决策的角度出发。虽然不同行业的业务不同，所产生的数据及其所支撑的管理形态也千差万别，但从数据的获取，数据的整合，数据的加工，数据的综合应用，数据的服务和推广，数据处理的生命线流程来分析，所有行业的模式是一致的。

如果在不同行业的业务和管理层之间，增加数据资源体系，通过数据资源体系的数据加工，把今天的数据和历史数据对接，把现在的数据和领导和企业机构关心的指标关联起来，把面向业务的数据转换成面向管理的数据，辅助于领导层的决策，真正实现了从数据到知识的转变，这样的数据资源体系是非常适合管理和决策使用的。

在宏观层面，大数据使经济决策部门可以更敏锐地把握经济走向，制定并实施科学的经济政策；而在微观方面，大数据可以提高企业经营决策水平和效率，推动创新，给企业、行业领域带来价值。

3. 大数据创新企业管理模式

今天信息时代机器的性能，更多决定于芯片，大脑的存储和处理能力，程序的有效性。因而管理从注重系统大小、完善和配合，到注重人，或者脑力的运用，信息流程和创造性，以及职工个性满足、创造力的激发。

在企业管理的核心因素中，大数据技术与其高度契合。管理最核心的因素之一是信息搜集与传递，而大数据的内涵和实质在于大数据内部信息的关联、挖掘，由此发现新知识、创造新价值。两者在这一特征上具有高度契合性，甚至可以标称大数据就是企业管理的又一种工具。因为对于任何企业，信息即财富，从企业战略着眼，利用大数据，充分发挥其辅助决策的潜力，可以更好地服务企业发展战略。大数据时代，数据在各行各业渗透着，并渐渐成为企业的战略资产。数据分析挖掘不仅本身能帮助企业降低成本：比如库存或物流，改善产品和决策流程，寻找到并更好地维护客户，还可以通过挖掘业务流程各环节的中间数据和结果数据，发现流程中的瓶颈因素，找到改善流程效率，降低成本的关键点，从而优化流程，提高服务水平。大数据成果在各相关部门传递分享，还可以提高整个管理链条和产业链条的投入回报率。

4. 变革商业模式

在大数据时代，以利用数据价值为核心，新型商业模式正在不断涌现。能够把握市场机遇、迅速实现大数据商业模式创新的企业，将在 IT 发展史上书写出新的传奇。

大数据让企业能够创造新产品和服务，改善现有产品和服务，以及发明全新的业务