第 1 部分

基 础 篇

第 1 章

绪　论

1.1　信用机制的发展与区块链的诞生

1.1.1　信用机制的发展

马克思的经典著作《资本论》中开篇明义地指出“信用即是有条件的信任”，由此可见，信用是借贷的一种特殊形式，到期偿还应额外支付一定报酬。马歇尔的著作《货币、信用与商业》对于信用的理解较为全面，涵盖了诸如借贷、信任、信誉等丰富的含义。信用一方面是一种借贷行为，另一方面又可以算是一种制度创新，在信用交易日渐普遍的过程中，一种新的交易规则或秩序就应运而生，信用关系也带来了金融市场的制度性变革。在信用产生后为减少失信行为的出现，各式各样的信用机制由此也逐步出现。通过建立信用关系、信用行为和信用制度三者之间的联系，通过制度约束使信用主体实现在信用关系中所产生的预期收益是信用机制的关键所在。

信用机制发展先后经历了由人格维持机制到抵押机制、信誉机制，最后到第三方保障机制的演变历程[1]。在现实商业社会中，大量第三方信用机构的存在就是为交易提供信用服务的。人类需要为信用付出极高的成本，就连税收的很大一部分也是用于社会化的第三方信用服务，如商检、质检、交易所、法院、仲裁、协会、担保、保险等，且大量的人力资源服务于第三方信用机构。

区块链作为一种较低成本的信用机制，一诞生就吸引了很多人的注意。区块链的信任来自于其底层技术，即用历史信息换得现行的信任。从密码学来说，一旦盖好时间戳，这个区块就没有办法被破解，也就是说所有的历史交易信息都在掌握之中，无法被篡改。

用时间换取人们的信任，这是区块链所带来的冲击与变革。同样地，如果政府能够在长时间的运行过程中做到信守承诺、说到做到，那么民众对政府的信任度也会增加。对于比特币来说，运行时间越久，被篡改的难度也越高，这是它的特点，也是由它的设计机制所保证的。区块链的出现可以减少甚至不再需要第三方仲裁、信任中介的参与，由数字资产的所有交易历史、参与者的共同监督来形成信用，在主体都为理性人的假设下，这种机制使得主体按诚实信用规则行事。具体来说，这种机制主要具备如下优点。

1.1.1.1　弱中心化

弱中心化是区块链技术的颠覆性特点，减少交易当事人之外的资源参与交易，达到节约资源、交易自主化、流程简单化的目标，排除被中心化代理控制的风险。传统的交易由于点对点都互不信任，因此必须依靠第三方信用的介入，区块链实现了在无中介机构的情况下双方相互转账，比特币就是迄今为止应用区块链技术最成功的数字货币实例。

1.1.1.2　点对点交易

点对点交易具有高效率、大规模、无中心化代理的优点，所有成员参与对价值传递的监督、控制和审计，包括地址、链、公钥、私钥、摘要等几乎所有数据记录的要素，具有全生命周期的信用连续性。同时，所有节点实时同步，谁也无法实现全局控制，且永不宕机。目前的区块链点对点交易系统主要有线上 P2P 交易、线上 B2C 交易和线下交易三种形式。

1.1.1.3　价值传递

信息传输效率提升很大程度上是因为信息可以实现无限复制，但信息无限复制却极大破坏了信息的价值传递。区块链技术的连通性、分布式等特征，使点对点沟通得以实现。另外，可追溯的特点让信息传递有迹可循，信息所有者的收益权和处置权得以保障。区块链可以完整、“不可篡改”地记录价值转移的全过程，这使得账本证明交易记录具有唯一性，即同一个标的物不可能同时卖给两个人，即避免“双花”问题。

1.1.1.4　合约的自动执行

将合约的规则由编程固化在代码中，能够自动判别节点执行合约的条件与义务，自动执行条件满足时的合约事项，能够在没有中心机构监督的情况下确保合约执行过程中的有序性与流畅性，减少资源浪费的同时提高执行效率。例如，合同条款规定一家公司债权发生转移的条件，转换为区块链中的编码，当条件发生时，智能合约执行定义的合同条款，避免人工干预的不可预期性。

1.1.1.5　自治性

区块链技术是使用多中心化共识维护的一个完整的、分布式的、不可篡改的数据库技术，其使用的统一的规范和协议（比如公开透明的共识算法）可以维护节点间数据的一致性，使数据得以自由、安全地在整个系统中的所有节点间实现传输与交互，且整个系统都能够在相互信任的环境下运行，从而巧妙地将对人的信任转变为对机器的信任，并且单一节点的干预几乎无法影响整个区块链。

1.1.2　区块链的诞生

大卫·乔姆是 20 世纪八九十年代密码朋克的“主教”级人物，他于 1990 年发明了密码学匿名现金系统 Ecash。乔姆认为分布式的、真正的数字现金系统应该为人们的隐私

加密。

1997 年英国密码学家亚当·贝克发明了哈希现金(Hashcash),并在其发现过程中使用了工作量证明(Proof of Work,PoW)系统。PoW 系统后来成为了比特币的核心理念之一。比特币区块链协议的原型之一是哈伯和斯托尼塔在 1997 年提出的一个用时间戳的方法确定数字文件安全的协议。时间戳最大的特点就是当一个虚拟货币被交易时,将被盖上时间戳,在那之后它就不能被篡改了。

密码学专家戴伟于 1998 年发明了 B-money,它强调了点对点交易和不可更改的交易记录,每一个在网络中的交易者都保持着对交易的追踪。

2004 年,PGP 加密公司的顶级开发人员哈尔·芬尼推出了电子货币"加密现金"并采用了可重复使用的 PoW 机制。但是他们单一的发明和设想还是不够成为一种世界型的虚拟货币。Ecash 于 1998 年宣布倒闭,工作量证明系统不能保证数字货币是否交易过很多次,时间戳这个技术协议只被政府小范围应用。B-money 系统中,戴伟并没有解决账本同步的问题。

2008 年,一切技术条件已成熟,时间条件也已成熟,比特币的开发者兼创始者中本聪(Satoshi Nakamoto)回答了之前的虚拟货币先驱们失败的原因[2]。他认为之前的虚拟货币失败最重要的原因是,都有一个中心化的结构,所有的交易数据都会汇总到公司的数据中心,和政府发行的货币没有任何区别。一旦有虚拟货币背书的公司倒闭或保管总账本的中央服务器被黑客攻破,该虚拟货币即面临内部崩溃的风险。中本聪通过对大卫·乔姆的 Ecash 进行一系列的优化创新,综合了时间戳、工作量证明机制、非对称加密技术以及未花费的交易输出(Unspent Transaction Outputs,UTXO)的结构,最终发明了比特币。

可见区块链并不只是一种单一的技术,而是上述多种技术的集合。而比特币仅为区块链技术首次大规模应用的典型案例。区块链为人们带来了一种新的选择,它完美地解决了记账过程中的互信难题。由于它是一个去中心化的分布式的账本,且不可篡改,因此可以在不需要任何第三方参与的前提下达成互信[3]。中心化与去中心化如图 1-1 所示。

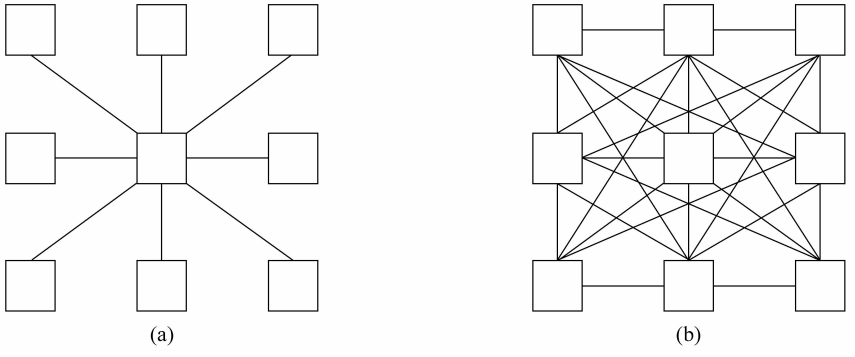

图 1-1 中心化与去中心化

(a) 中心化;(b) 去中心化

1.2　从信息交换到价值交换

互联网交换的是信息，区块链交换的是价值。利用互联网获得和交换信息已成为社会的一个非常重要的特征，因此，过去的互联网时代常被称为信息互联网时代。但与此同时，信息安全问题也日益突出，网络入侵、信息泄露及网络犯罪等案件也日益上升。因此，互联网作为信息交换的中介，已经不能完全满足现代社会的需求。信息交换到价值交换的转变是大势所趋。区块链的迅速发展则为此改变带来契机。

区块链技术可创新性的实现不需要中介信任的价值交换。区块链是以对等网络为基础的分布式账本系统解决策略。分布式存储应用在其数据当中，兼具“时间顺序、前溯验证”特性的信息块组成的链式结构形成了其逻辑结构，时间段内的交易集合附加时间戳形成了它的每个信息块。点对点交易、私密交易、可审计交易、智能交易都可以通过其实现，从而建立了以区块链信任为基础的无需中介的价值交换。区块链技术能够实现价值交换的原因在于其有以下特点。

1.2.1　共享账本

分布式记账[4]是区块链的本质，系统中相关节点都参与了对发生的每笔交易的确认和区块的生成验证、协调和同步，进而让各节点账本具有准确性和一致性。区块账本被多个节点完整保存，交易前的价格的制定和风险的识别以实现共享账本嵌入信用管理为基础，各参与方通过共享账本自行完成交易撮合，之后再进行快速结算并且能省略对账和审查环节。账本可以多方共享，也可以设置为私有、公共或者半公开。

1.2.2　点对点交易

区块链中所涉及的点对点交易的信任问题实际上是通过数学途径解决的。其中，所有权信任问题通过数字签名解决，信息真实性和完整性问题通过非对称加密解决，价值转移过程中的信任溯源问题由 UTXO 设计结构解决，信任强制自动化执行问题可以通过智能合约解决，并在机器之间以共识算法为核心建立信任且同时完成信用创造。过滤或者延迟交易无法发生在任何中介当中。最终，点对点交易后，共享账本中记录信息的真实性、客观性和不可篡改性才得以保障。

1.2.3　私密交易

密码学中的哈希算法能够在不需要看到明文信息的情况下验证某组信息是否被篡改过[5]。这就完善了在不知晓具体交易内容的情况下非交易节点涉及点对点交易验证的问题。并且，由于商业往来占据价值交换的大部分，价值交换需要有交易路径、交易内容隐私保护，更细粒度的隐私保护通过区块链中的密码学设计实现，更有针对性的保障出现在对交易主体和业务内容的保护，价值交换也真正具有了便利性、安全性和可操作性。

1.2.4 智能交易

以区块链技术为核心的智能合约，能够自动执行不依赖第三方的双方协议承诺条款，当预定设定后具有不变性和加密安全性，并且透明可信、自动执行和强制履约也是其特点。网络中各对等节点进行自动交互并且完成高效合作的过程，可以由智能合约来实现，无须耗费支付给中介的达成信任的成本[6]。区块链技术不能篡改、不能人为干预的特性，正好拓展了智能合约的应用场景，随着智能合约越来越广泛地应用，能够在极大程度上降低交易成本。通过智能合约的形式体现和表达商业逻辑，也成为了许多人使用的方法，对实现范围更大、成本更低的新协同机制起到促进作用。智能合约模型如图 1-2 所示。

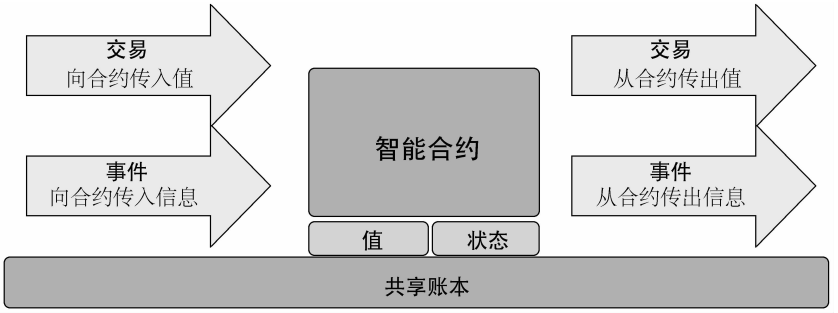

图 1-2 智能合约模型

1.3 区块链技术面临的挑战和机遇

1.3.1 区块链技术面临的挑战

经过十余年的发展，区块链取得了长足的进步，集中表现为结合数字货币的公链、以产业和业务结合的联盟链、企业内部使用的私链等三种主要形式。然而，区块链技术在蓬勃发展的同时，也面临着一系列挑战（见表 1-1）。

表 1-1 区块链技术面临的挑战

挑　战	描述（以供应链为例）
合作伙伴之间的协作水平	跨多个不连贯的供应链参与者之间的协调流程和数字化转型具有挑战性。全球供应链涉及许多参与者（生产者、经纪人、运输商、加工者、批发商、零售商和消费者），彼此不信任和不愿共享数据限制了协作水平。
各个参与者的连通性水平和数字成熟度水平	区块链技术需要互联网连接和数字素养才能被广泛采用；在某些新兴市场和农村地区互联网基础设施较落后，人们的数字素养有待提高。
数据协调流程成本高昂	随着业务扩展到多个国家/地区，可能难以跟踪库存并管理众多数据和法规要求。努力跟踪和核对单笔交易中来自不同监管环境中的大量数据时，需要协调这些数据。在许多情况下，这些对账过程仍然是手动的。

续表

挑　战	描　述
需要监管框架	区块链的智能合约可以更有效地管理边境程序和国家单一窗口，并提高贸易数据的准确性。真正的挑战将是解决互操作性问题和标准化，以及建立有利于无纸贸易的监管框架的政治意愿。
安全问题	尽管由于区块链的分散和分布式性质以及使用加密技术，它们与传统数据库相比具有很高的弹性，但它们不能完全免受传统安全性挑战和技术进步的影响。
有利的监管框架	需要一个能够识别区块链交易的合法性，阐明适用法律和责任，以及规范数据访问和使用方式的监管框架。最关键的问题与区块链交易的法律地位有关。承认电子签名、电子文档和电子交易（尤其是区块链交易）有效性的立法至关重要。
资料私隐	数据隐私和数据本地化，对跨境数据传输的限制以及数据隐私的问题，越来越多的国家采取对数据流施加要求或限制的措施。
维护基于区块链的系统的成本	需要仔细考虑过渡到和维护基于区块链的系统的成本。从区块链中获得的大部分成本削减可能与技术本身无关，而与迁移到区块链系统所需的集成和精简工作有关。
可扩展性挑战	由于预定的区块大小和能源消耗问题，区块链的可扩展性有限。对于公共区块链而言尤其如此，但对于私人区块链则没有相同的限制。

1.3.1.1　挖矿能耗

比特币和以太坊以及其他多个主流公链均使用工作量证明作为共识算法，同时对取得记账权的节点进行奖励。以比特币为例，其工作量证明使用特定的哈希函数计算一个随机数，为了保证难度，要求结果随机数的前若干位为 0。由于过去几年中虚拟货币价格出现了连续强劲上升势头，大量计算资源被投入到挖矿计算之中，并且出现了以比特大陆为代表的行业巨头。

如果把全部挖矿的计算能力折算为浮点运算，粗略估算的总体计算能力达到 1 023FLOPS(Floating Point Operations Per Second)，已经达到谷歌计算能力的 100 万倍，或者全球 500 强超级计算机总体计算能力的 10 万倍。如此庞大的计算能力当然以电力消耗作为基础，其总用电量已经超过世界上 160 多个国家。

事实上，2018 年 *Nature Energy* 的一篇文章指出比特币挖矿的能源损耗超过了黄金、铂金等贵金属，1 美元比特币消耗的电能实际上能够开采 3.4 美元的黄金。然而，挖矿使用的电能对虚拟货币之外的世界全无意义，在全球可持续发展的大背景下尤为刺眼。

1.3.1.2　可扩展性

无论作为虚拟货币账本还是广义的数据库，区块链上的数据服务均以交易形式完成。由于区块链的分布式特性，交易总是并发产生的。因此，区块链的可扩展性一般指单位时间内能够支撑的最高并发交易个数。一般来说区块链交易的吞吐率可以用每秒交易量(Transactions Per Second，TPS)来表征，其计算方式为

$$\text{TPS}=\frac{\text{一个区块内包含的交易数量}}{\text{区块产生时间}}=\frac{\text{一个区块内包含的交易数量}}{\text{共识算法运行的时间}+\text{广播并验证的时间}}$$

也就是说，TPS 由数据块的大小、共识算法运行的时间和广播并验证的时间共同决定。值得注意的是，由于区块链采用去中心化方式验证交易，因此必须在多数节点形成共识之后才能完成验证，其后果就是目前的区块链在节点增加的情况下交易速度必然下降。比特币和以太坊在创建之初就优先考虑去中心化和安全性，这一策略一定程度上牺牲了其可扩展性。比特币的吞吐率为 3.37TPS，以太坊略高，但也只有 30TPS 左右。当前还有一些新诞生的区块链项目选择为了可扩展性而牺牲去中心化程度和安全性，并且尝试以这种策略启动网络，这些“后起之秀”采用的策略的有效性仍有待观察。迄今为止，尚未发现一个能完美结合去中心化、可扩展性和安全性的方案，而这些特性都是建立一个大规模的功能完备的加密货币网络所必需的。

1.3.1.3 安全性

区块链的交易具有可靠的安全性，因为交易过程中的数据记录会根据时间的顺序进行记录。相应的时间和发生顺序都会记录在每个区块中[7]。这样针对不同的交易都可以进行追踪查询。任何人都不能对其中的数据进行篡改。并且修改的概率小之又小还过于烦琐。因而，对于区块链的信息记录有很高的安全性。

由于区块链技术基于去中心的方式运行维护，使得每笔交易都需要通过全网广播对其他节点进行发布，降低了之前存在于中心数据库的篡改风险。当出现数据不一致时，可通过信息的节点数量判断其真伪，即只有至少同时篡改 51%的节点数据后，单笔数据才能被篡改。这使得之前篡改单一节点的攻击数据中心方式不再有效。如果要同时篡改半数以上节点，这会对算力与成本有极高的要求，从而能更大概率地保证数据安全[8]。

区块链采用了去中心化的共识机制，本身的安全性是比较高的。然而，区块链由网络实现，因此其网络协议的各个层次均有可能受到攻击。例如，Mt. Gox 交易所曾因为钱包的安全性漏洞被盗走 3.6 亿美元，直接导致交易所破产。

更为严重的安全隐患来自于智能合约。由于智能合约是具有图灵完备性的程序，因此其行为更加复杂，而且代码在分布式网络环境上运行时，潜在风险会大大提升。目前的智能合约编程以 Solidity 语言为主，该语言成熟度相对较低，因此虽然代码由虚拟机执行，但攻击者可以利用溢出等情况侵入宿主电脑。同时，为了支持交易引入了跨合约程序调用等功能，易于遭受重入攻击。典型案例是以太坊上的众筹项目 DAO，它在 2017 年遭到黑客攻击，被盗走当时价值 6 000 万美元的以太币。

区块链的智能合约可以写入自动执行的合约条款，有助于多方参与者根据事先约定规则处理交易、结算的事务，从而完成数字资产交割和转移。此外，区块链共识机制和智能合约共同构建了去中心化环境下的数据生成、传输、计算和存储等一系列规则协议，为以数据为载体的数字内容作品和资产价值的安全流动创造了条件。由此，可实现价值转移基础协议，便于交易、消费和流转。

1.3.1.4 易用性

将区块链等价于比特币，这是目前的误区之一。实际上可通过在算法中内嵌逻辑结

构的方式规范交易流程以实现分布式记账。全网广播的模式在一定程度上提高了违约成本，同时也提高了信任度。而由于金融衍生品日渐复杂，其内涵条款逐渐增多。由于托管机构与资产提供方存在着利益关系，托管机构未必能及时反映基础资产价值波动状况。可凭借区块链的可操作性为产权情况和金融资产价格变动设定业务逻辑，这可以保证相关资产的交易合规性得到保证，为投资者实时监控基础资产动向提供便利[9]。

智能合约的引入使得区块链在应用领域上升到全新的层次，形成了人类商业行为的一次革命。但智能合约以程序形式体现，对一般用户来说具有一定难度。在传统的线下世界，大多数人都可以看懂合同内容，相当比例的用户则可以在律师指导下或参照模板编写简单合同。智能合约则不然，要求用户必须具备编程能力才能撰写合同，无形中又限制了其应用范围。

1.3.1.5　隐私保护

在大数据时代，保护数据隐私的重要性不言而喻。目前区块链公链上的数据大体来说是完全开放的。因此，随着区块链应用的不断拓展以及其数据库应用比重的提升，如何在区块链上引入完备的隐私保护机制已经成为亟待解决的问题。

区块链的形成使得交易双方实现匿名化。计算机的算法实现了去信任的直接交易模式。区块链交易方法极大地保护了个人隐私，因为交易双方的传递地址都是通过共同的公共地址进行交易的。所有数据公开，任何人都可以共享区块链上的数据。但交易双方的资料并不公开[10]。

1.3.2　区块链技术面临的机遇

针对区块链面临的主要挑战，人工智能（AI）能够为应对其中一些挑战提供新的思路，特别是在智能合约处理和挖矿函数设计上潜力极大，也有人认为 AI 能够为区块链提供自动治理能力。人工智能为区块链带来如下机遇。

1.3.2.1　安全验证

区块链的安全需要对各个网络和应用层次进行综合保护才能实现，尤其是智能合约的安全性。由于智能合约属于软件代码，因此传统式软件缺陷和安全漏洞可以通过形式验证（Formal Verification）的方法处理，近年来基于机器学习的漏洞模式检测手段已经出现，一些工作证明了可以把抽象语法树作为递归神经网络的输入进行有无漏洞的检测。同时，智能合约在分布式网络上以并发方式执行，因此需要在沙箱网络上引入动态攻防手段，验证动态安全性。在动态攻击过程中，除了使用已知攻击方式外，当前的生成式网络也运行自行产生攻击方式。实际上，目前正在蓬勃发展的对抗式生成网络提供了将合约和攻击放在统一框架之内进行全面优化的可能性。

静态验证是对源代码或字节码（Byte Code）直接进行分析（不需要执行代码），分析工具目前以形式验证（Formal Verification）为主，但基于深度神经网络的机器学习方法也在快速出现。形式验证是在硬件验证的基础上发展起来的，目前已被广泛用于软件安全验证。其手段是把程序表示为一定的形式化模型（即基于时序逻辑的数学模型），然后用数

学方法证明其正确性。

形式验证的方法可以分为符号执行(Symbolic Execution)、模型校验(Model Checking)和定理证明(Theorem Proof)三大类。符号执行算法遍历代码的所有可能执行路径,并提炼出每条路径的状态转移与相应条件,并检查每一路径上是否可能存在违反约束的反例。模型校验把程序表示为逻辑模型,把针对某一安全漏洞的安全条件表示为相应的属性,然后使用可满足性求解器来寻找是否存在违反该属性的输入数值,如果存在,则表示代码存在漏洞,否则表示代码一定满足该属性。定理证明比模型检查的能力更强,能够做函数级别的检查,但一般需要专家级别的人工干预。

虽然形式验证不属于人工智能技术,但 AI 确实能够在很多方面提高形式验证的性能。事实上,形式验证技术为了解决状态爆炸问题而引入了大量的启发式算法,AI 能够找到更优化的启发条件。另一方面,把源代码表示为抽象语法树后,完全可以利用递归神经网络的模式提炼能力进行安全漏洞检查,目前这方面已经有一些成功的工作。

相对于静态验证,动态验证需要在分布式不可信环境下的动态程序执行过程中发现潜在漏洞,其难度更高。一般来说,此时需要对智能合约进行"沙箱"仿真,即在测试链上执行代码,以人工方式注入攻击。当前快速发展的生成对抗网络(Generative Adversarial Networks)提供了在小量攻击范例的基础上自动产生攻击代码的可能性,有望为智能合约安全性提供新的工具[11]。同时,AI 技术也可以和智能合约虚拟机结合,进行动态漏洞嗅探。与静态检查不同,动态检查一般不需要在源代码中精确定位潜在漏洞,因此解释性较差的深度学习技术具有更好的可行性。

1.3.2.2 智能合约代码生成

对智能合约,可从以下几个方面进行理解:第一,智能合约是一段复杂的链上代码,由此成为区块链编程特性的基础;第二,智能合约是系统账本不可缺少的组成部分,它始终按照预先设定的程序运行;第三,智能合约是具有法律文件性质的代码程序而不是一般的代码程序,一旦所有条件都满足,智能合约将自动产生合法交易;第四,人们的行为在未来可通过智能合约来约束,可编程社会很可能成为智能合约的终极应用[12]。

智能合约表现为使用编程语言撰写的程序,因此使用门槛较高会严重影响智能合约的可用性。不具备编程能力的一般用户必须聘请程序员完成合同编制工作,但是 Solidity 现有社区规模较小、编程人员不足。人工智能技术提供了自动综合代码的可能性,当前以微软 DeepCoder 为代表的深度神经网络已能够在专用领域根据一组示例自动产生代码。

值得注意的是,虽然与针对任意问题的自动化代码生成的距离仍然遥远,但智能合约本身已经呈现出许多显著特色,例如,程序具有比较清晰的状态(可以用有限状态机表示)、计算过程相对简单(主要是针对虚拟货币的算数运算)、存在典型模式(例如存取款、投票、彩票等),使得针对性的代码生成具有较强的可能性。

智能合约代码生成工具流程起始于以简单脚本语言、图形化方式甚至自然语言捕捉的交易意图,然后通过机器学习工具抽取交易关键特征并对交易进行分类,在此基础上结合智能合约设计模式进行代码综合。代码生成工具还可以进一步与安全验证工具结合,进行迭代式自动攻击和代码修订,从而最大化实现安全性。

1.3.2.3　AI 挖矿函数

挖矿是一种通过消耗计算机资源来提高恶意节点攻击网络成本的方式。挖矿的中心思想起源于 Hashcash 机制，该机制初次提出时主要用来阻止恶意用户向邮件服务器发送垃圾邮件[13]。任何用户在向邮件服务器发送邮件的时候，都必须在邮件中加入一些随机字符，然后得出邮件内容的哈希值，只有当哈希值小于设定值的时候，邮件服务器才能接收请求。如果用户需要发送一封邮件，则必须花费一点时间找出一个随机字符使整个邮件被邮件服务器验证通过。虽然在一定程度上会影响正常用户的发送速度，但影响是微乎其微的，无论是合法用户还是恶意用户，都无法绕开这个过程。而恶意用户为了大量发送垃圾邮件，就不得不大量计算满足条件的值，这无疑会增加恶意用户的攻击成本，这就是中本聪设计比特币的时候，需要矿工计算区块哈希值的原因[14]。

中本聪为比特币设计了非常精巧的挖矿函数，即根据块内交易的内容使用单向哈希函数计算满足特定要求的随机数。一般说来，挖矿函数应该具有以下特点：①函数具有单向性，即计算结果难度较高，无法直接猜测，但验证结果的正确性却很容易；②函数计算应具有一定强度，同时难度可以调整；③计算该函数时不需要传递大量数据，即不会给区块链网络带来额外带宽负载；④函数应具有公平性，也就是说，算力强的节点只是拥有较高概率获得奖励。除此之外，挖矿函数应具有增值性或公益性，即挖矿能够产生虚拟货币之外的价值。事实上，当前 AI 应用面临算力不足的困境，如果能够通过区块链的奖励机制吸引算力投入，的确可以获得事半功倍的效果。

从提供算力的角度看，显然训练深度神经网络等机器学习模型的实际意义最大。不仅如此，训练过程也确实具有单向性，即训练过程强度高，但是验证过程（即对已知结果数据做一次推断）强度很低。不过，深度神经网络的训练难度很难预测，因此也不容易控制，而且训练时一般需要传递大量的训练样本数据，网络传输压力很大。由此可见，深度神经网络的训练过程作为挖矿函数仍具有很大困难。

另一个可能的 AI 挖矿函数是马尔可夫链蒙特卡洛（Markov Chain Monte Carlo，MCMC）算法。MCMC 在贝叶斯学习和推理中具有极其重要的作用，入选 20 世纪十大算法之一。该算法是从已知概率分布的随机数出发，产生针对特定后验概率分布的随机数并推测该分布的特性。MCMC 具有单向性，难度相对可控。但是，MCMC 作为挖矿函数的缺点是在验证时需要传递比较大量的数据。Matrix AI 区块链提出了一种新的基于深度学习的挖矿机理，其来源是针对深度神经网络的对抗攻击。

1.3.2.4　区块链自动治理

任意复杂系统在全生命周期过程中都要经历自身和环境的变化，因此需要一组规则决定在变化发生时怎样对系统自身进行改变。规则可以体现为代码（例如智能合约）、法律、过程（例如 X 发生时必须执行 Y 动作）和责任要求。系统治理就是创建、更新和放弃这些规则的决策过程。由于区块链的去中心化特点，其治理过程涉及平衡开发者、矿工、用户和商业实体的利益平衡。

区块链可被描述为具有时间戳的公共交易记录，并通过分散的“矿工”的计算工作得

以加强，这是仅仅从技术层面来看的。这种公共记录通常被称为“通用账本”“分布式账本”或“公共账本”。区块链能够发挥治理功能的核心特质包括两个方面：一是区块链系统的分布式存储，区块链是一种数字化存储的、公共的、人们可以据以与他人订立合同的分布式账本；二是区块链系统的可自动执行，区块链可以通过计算审查来自动执行已验证的交易或合同[15]。

区块链系统传统上采用离线治理方式，即任何人均可以提出改变治理规则的建议[16]。然而，是否采纳某项建议，则需要按照一定的协议对建议进行评估，最后通过多方投票的方式决定最终决策并修改相关代码上线执行。比特币的相关治理通过 BIP (Bitcoin Improvement Proposal)协议进行，虽然决策速度较慢，但是很多人认为相应的渐变过程对比特币的可持续发展是有利的。另外，目前也有不少人认为基于人工智能的自主、在线治理更适合于高速变化的网络环境。在这种情况下，治理过程可以通过基于 AI 的增强式学习实现，DFINITY 区块链甚至提出使用 AI 代理作为用户代表自动进行投票。治理过程的人工智能化确实能够带来一些好处，特别是在处理细粒度的纠纷处理(例如挖矿或者交易作弊)时效率可以很高。然而，近来的研究结果表明，由于目前 AI 技术大多基于人类标注样本，因此同样可能存在偏见，所以 AI 决策可能并不像很多人所想象得那样公正。同时，AI 决策体现为 AI 模型和算法，一般用户很难理解，而且其安全性和公正性的验证也是很困难的问题。

1.4 全球区块链投融资分析

伴随着当今时代区块链技术的迅猛发展态势，越来越多的投资者开始青睐以区块链为主要行业的企业，所以在区块链相关的市场中有许多的投资与市场活动在进行着。有数据显示，2009 年以来已经有超过 13 亿美元的高额资金注入区块链相关企业。进一步细看与思考，会发现，像 21Inc、Bit Fury 等与比特币相关企业被推到了投资风口，当然与此同时，也有像 Blockchain、Blockstream、Ripple 和以太坊等专注基础设施的企业得到融资。不难看出这是行业发展初期和兴盛期都会有的特点，企业在有了这么多的资本以后，肯定会得到快速成长。然而，就目前而言，大家的目光开始逐渐放在了区块链技术上，资本也跟着转移到了区块链技术上，所以还有很多小型初创的区块链企业有很大的待挖掘空间。目前，21Inc 这家计算机硬件公司，自 2013 年以来已经累计获得 1.21 亿美元的投资，其次就是 Coinbase 公司，获得了 1.05 亿美元的投资。

近年来，人们往区块链企业投入的资本不断增加。通过数据发现，大部分企业在获得了大量资金投入后，往往蛰伏长达 11 年之久，才在市场上崭露头角。然而，再仔细观察，就会发现，完成了第三轮融资的公司却只有 Bit Fury、Circle 和 Coinbase，其他大部分公司还处于早期的几轮融资阶段，这说明还有大量潜在的未来投资商机与发展机会。下面对全球区块链投融资现状进行分析。

1.4.1 主要的投融资领域

根据 2013 年至 2016 年 4 月全球区块链行业投融资项目类型分析，目前最多的投资

领域是矿机芯片、交易平台等与比特币十分密切的领域。相对而言，这些领域更加成熟，参与的企业更多，创立的时间也更久。其中，挖矿领域是一个投资相对最多的行业。但是，上述统计主要为欧美矿机行业的投资行为。根据实际情况来看，考虑到在中国大陆地区有更多的矿机厂商和矿场投入，应该有更加集中的资金投入。但是中国地区的这些投资信息大多数都没有公布出来，因此无法知道真实的投资情况。不仅国内如此，大多数矿机和矿场的资金投入，主要都是来自自筹资金，而目前大陆地区比特币算力占全球总算力的 70%，所以可以推断出矿机和芯片之类的总投资额，至少是目前统计数据的 2 倍到 5 倍[17]。

作为比特币的底层技术支持，区块链本质上是一个去中心化的分布式数据库，该数据库由一串遵循密码学规则的数据区块有序连接而成，区块中包含着无法被篡改的数据记录信息。由于其具有透明性、匿名性、自治性、去中心化、信息不可篡改等特征，所以在其他很多领域还存在许多的别的细分，比如智能数据分析、物联网、身份认证、数据认证、社交通信等。这些领域或者建立在比特币区块链基础之上，或者建立在区块链应用基础之上(如以太坊)，这些比较早期的项目，大部分其实还是在种子轮或者还比较早的投资阶段。

1.4.2　不同国家/地区的投融资差异

同样考虑 2013 年至 2016 年全球区块链的行业投资与融资项目的类型，可以发现目前统计的投资数据总量是在不断增长的。在 2012 年，几乎没有太多的公开投资情况出现，但到了 2015 年，众多的投资事件相继出现，并覆盖了区块链行业的多个领域[18]。

同时发现，在每年的投资中，北美洲占据了主要份额，有大量的投资都集中在北美洲，而欧洲紧随其后，然后才是亚洲。在北美洲，由于技术与人才方面的支持，很多的技术人员基本上可以直接提出核心的理论与方案并实施。在这方面，其他地区要远远落后于北美地区。

从比特币到区块链，目前其实还处于一个初级的发展阶段，主要还是集中在技术的基础架构建设中。而纵观整个 IT 技术的发展史，在基础架构领域，基本都是以欧美为主的。无论是 UNIX、DOS、Windows、Linux 还是 Android，这些基础操作系统或者数据库系统，都需要有对 IT 技术有着深刻的远见和庞大的资金投入，以及大规模技术基础才能够进行开发。而亚洲地区在这一领域始终没有太多的话语权。到了比特币和区块链阶段，无论是基础理论还是最早原型设计，也都是在欧美开始的，因此，亚洲难以在这方面有机会全面超越欧美地区。

但是，必须要指出一点的是，在早期阶段，亚洲大多数国家对于比特币并不持有友好的态度。中国曾明文规定，禁止所有金融机构和支付机构开展比特币等数字货币相关业务。而早期全球最大的比特币交易所 Mt. Gox 在日本因为遭受黑客攻击而倒闭，并因此产生了一系列诉讼行为，所以日本政府对于数字货币的态度也一直非常冷淡，而且希望对此进行严格监管。在未来政策上的态度不明确，必然会造成投资事件和金额远远低于正常的情况，或者造成许多投资事件不愿意公开披露。

正如前面所指出的，中国大陆地区、在比特币矿机和芯片方面的投资情况，如果把这

些从未披露的投资数据都计算在内，也许不会低于欧洲方面的投资数据。截至 2016 年 5 月，2016 年的投资数额已经超过了 2015 年整年投资数额的一半，因此 2016 年整年的投资数额超过 2015 年应该是大概率事件。有理由相信，区块链行业相关的投资将在未来变得越来越频繁。

有个有趣的现象是，尽管从 2015 年下半年开始，“区块链”概念被视为在未来会获得越来越多的重视，许多相关会议和金融媒体都在密集地讨论其可能带来的颠覆式影响，甚至认为“区块链”技术已经被炒作过度，甚至可能有泡沫产生。但是从投资数据来看，并没有出现极大幅度的增长，完全是一个线性增长方式。从这一点来看，无论“区块链”这个概念被如何热炒，投资数据完全表现的是一种行业初级发展的特征，没有任何出现指数级增长的“泡沫现象”。

考虑到区块链技术的不确定性在未来的各行各业中的运用与发展还会存在，再加上当前大部分工作还只是在探索一个底层架构，所以其实仍然有相当多的投资机构在观望。当然，等到局势更加明朗以后，投资机构可能会大张旗鼓地涌入这个行业。

不同于在互联网发展早期，许多新的技术和创新都是由初创公司开始的，许多大型公司都是扮演投资者和并购者的角色。由于区块链要获得大规模应用，最容易的方式不是推翻目前所有的金融场景，而是帮助现有金融场景降低成本或者提高效率。因此许多区块链的研究和开发活动，都是在大型金融机构内部进行的。因为只有它们有更加合适的应用场景，并且明白自己的需求和痛点所在。然而，它们的具体进展和投入都没有对外公开，所以这方面的许多数据无法从公开渠道中获得。

根据目前的线性增长趋势来判断，类似于 1995—1996 年的互联网投资情况，距离 2000 年的全球互联网泡沫的高峰形态相去甚远。因此，区块链行业投资在未来还有巨大的上升空间。

据零壹数据统计，2018 年全球区块链领域共获得 451 笔融资，总计约 333.5 亿元。全球区块链领域种子或天使轮融资共有 196 笔，A 轮（含 Pre-A、A、A＋）共有 71 笔，合计占所有轮次的 57％；共获得 175 笔战略投资，涉及金额为 107.8 亿元。中国、美国、新加坡融资合计占全球总数的 83.1％。其中，单中国就获得了 266 笔融资，总额为 154.7 亿元，占全球融资 46.4％，占总数第一，笔均 0.6 亿元；美国共获得 80 笔融资，共计 114.7 亿元，列居第二，笔均 1.4 亿元。随着技术在实体经济中逐渐落地，区块链受到的关注度也在大幅提升，特别是在金融科技融资领域，区块链一跃成为 2018 年之最。

1.4.3 不同年度的投融资重点差异

投资机构对于区块链在不同时间和不同领域具有不同的兴趣点。根据对 2013 年至 2016 年 4 月融资额超过 1 000 万美元项目进行分析[19]，投资者在早期更多地关注矿机芯片和钱包服务，显然这都是和比特币密切相关的，从 2015 年之后，开始把关注点转移到支付汇款、底层架构和技术服务上。这本身说明，投资者开始不再把所有的投资重点放在比特币上，而是开始重点建设整个生态环境。

有趣的是，对于交易平台的投资始终比较持续。可能不论未来区块链是何种走向，哪些区块链项目将会崛起，交易所始终会是打通数字货币和法币之间的桥梁。区块链行业

本身在快速发展中，体量也变得越来越大，必然会需要更多类似于桥梁这样的配套措施。所以，相信在未来还会出现更多的数字货币交易所。随着时间的推移，投资重点的确发生了不小的变化。很显然，从比特币时期的投资矿机和钱包之类，开始更多地形成以区块链技术为核心的完整生态系统。

另外一个比较明显的特征是，行业细分类型开始越来越多，会有很多围绕着核心生态系统的衍生产业逐渐诞生。尽管这些细分行业还十分弱小，但是能够看出，区块链已经在更多的细分行业获得资本市场的认可。根据国际会计师事务所毕马威发布的最新统计报告，可以得出：2018 年全球金融科技融资为 1 118 亿美元，较 2017 年的 508 亿美元激增 120%。2018 年，监管技术和区块链成为香饽饽，其中监管技术吸引的投资飙升 3 倍，由 2017 年的 12 亿美元增至 37 亿美元；而区块链投资同样保持迅猛势头，吸引投资 45 亿美元，略低于上年的 48 亿美元[20]。

本 章 小 结

本章为区块链技术及应用发展的绪论。首先介绍了信用机制的演化以及区块链诞生的背景，接着从价值交换的角度介绍了区块链技术能实现价值交换的原因，然后分别介绍了区块链技术所面临的挑战和机遇，最后从领域、地域、年度等方面对全球区块链投融资现状进行整体分析。

习　　题

1. 区块链信用机制主要有哪些优点？
2. 区块链技术能够实现价值交换的主要原因是什么？
3. 区块链技术面临哪些挑战？
4. 人工智能为区块链带来了哪些机遇？