



金融科技应用
金融服务与管理



“十四五”职业教育国家规划教材



国家职业教育金融科技应用专业教学资源库配套教材

职业教育国家在线精品课程配套教材

高等职业教育财经类专业群 **数智化财经** 系列教材

金融科技概论

主编 郭福春 吴金旺

中国教育出版传媒集团
高等教育出版社

2.5 区块链

2.5.1 区块链的概念和内涵

2008 年, 中本聪发表了论文《比特币: 一种点对点的电子现金系统》, 文中阐述了基于 P2P 网络技术、加密技术、时间戳技术、区块链技术等电子现金系统的构架理念。这篇论文堪称区块链技术和加密数字货币发明的基础。

2009 年 1 月 3 日, 中本聪创建了第一个区块(创世区块)。创世区块里, 中本聪留下一句永不可修改的话, 这句话作为“时间戳”被永远地留在了“创世区块”中。

区块链是一种“去中心化”的数据库, 包括一张被称作“区块”(Block)的列表, 其中每个区块都含有一个“时间戳”(Timestamp)、一条与前一个区块的“链接”(Link)和交易数据。随着区块链技术的不断升级, 业界将其演进发展历程分为三个阶段。

(1) 区块链 1.0(可编程货币): 去中心化的数字支付系统, 无障碍的价值转换, 以比特币为应用典型, 实现了数字货币的发行和流通, 功能相对单一。

(2) 区块链 2.0(可编程金融): 以智能合约的应用为特征, 通过智能合约推动多业务系统的协作, 扩展了区块链应用领域, 如股票、清算、私募股权等众多金融领域。

(3) 区块链 3.0(可编程社会): 将实现与物联网、云计算等技术融合发展, 试图在大规模协作领域提高行业的运行效率和管理水平。以上三个阶段并非依次实现, 而是共同发展, 相互促进的过程。

2.5.2 区块链的特征

从技术的角度来看, 区块链并不是一种单一的技术, 而是多种技术整合的结果。这些技术以新的结构组合在一起, 形成了一种新的数据记录、存储和表

达的方式。

区块链具有以下特征。

(1) 开放、共识。任何人都可以参与到区块链网络，每一台设备都能作为一个节点，每个节点都可以获得一份完整的数据库拷贝。节点间基于一套共识机制，通过竞争计算共同维护整个区块链。任何一个节点失效，其余节点仍能正常工作。

(2) 去中心、去信任。区块链由众多节点共同组成一个端到端的网络，不存在中心化的设备和管理机构。节点之间数据交换通过数字签名技术进行验证，无须互相信任，只要按照系统既定的规则进行，节点不能也无法欺骗其他节点。

(3) 交易透明、双方匿名。区块链的运行规则是公开透明的，所有的数据信息也是公开的，因此每一笔交易都对所有节点可见。由于节点与节点之间是去信任的，因此节点之间无须公开身份，每个参与的节点都是匿名的。

(4) 不可篡改、可追溯。单个甚至多个节点对数据库的修改无法影响其他节点的数据库，除非能控制整个网络中超过 51% 的节点同时修改，而这几乎不可能发生。区块链中的每一笔交易都通过密码学方法与相邻两个区块串联，因此可以追溯到任何一笔交易的前世今生。

2.5.3 区块链的关键技术

1. P2P 网络技术

区块链问世之前，分布式的 P2P 对等网络已经很成熟了。比如在网上下载视频，就是依赖这种点对点的网络传输协议。P2P 网络是整个区块链的基础计算架构。在区块链分布式网络中，中央服务器的概念被弱化，也就不再需要任何中心枢纽。网络中的各个节点都可以作为一个独立的个体存在。这些节点既能作为提供服务的服务器，也能作为发送请求的客户端。它们不再需要服务器的桥接就可以直接交换资源：从一个节点上发出的信息经过验证被发送到周边相邻的节点，而每一个相邻节点又会将交易发送到其他的相邻节点，最终扩散到区块链网络中所有的节点上，从而实现用户与用户之间资源的直接分享与利用。P2P 网络技术的特性保障了区块链技术是一个分布式的、去中心化的系统。

2. 加密技术

区块链使用的是非对称加密算法。非对称加密也就是加密一条信息实际上不是用单个密钥，而是用公钥和私钥两个密钥，他们可以保证在分布式网络中点对点信息传递的安全。

公钥是全网公开可见的，所有人都可以用自己的公钥加密一段信息，生成一个哈希值，来保障信息的完整性、真实性、并保证信息传递双方在不用信任

的网络上安全地传递密钥。

私钥是不公开的。信息拥有者要高度保护私钥的安全，因为被公钥加密过的信息只有拥有对应私钥的人才能解密。具体来说，这种非对称密钥的工作原理是，在区块链的信息传递过程中，信息发送方使用私钥对信息签名、使用信息接收方的公钥对信息加密；信息接收方使用对方公钥验证信息发送方的身份、使用私钥对加密信息解密。公私钥加密与解密的成对出现保障了信息的完整性、一致性、安全性和不可篡改性。

除了非对称加密算法之外，在密码学技术里，还有非对称的数字签名技术、保证数据唯一性的哈希技术、保护信息传递双方敏感信息的隐私保护技术和包括防攻击、身份认证、授权等在内的安全技术。基于密码学产生的安全技术是区块链的核心安全技术。

时间戳服务器经常用来进行比对以及验证处理，时间戳服务器是一款基于PKI（公钥密码基础设施）技术的时间戳权威系统，对外提供精确可信的时间戳服务。它采用精确的时间源、高强度、高标准的安全机制，以确认系统处理数据在某一时间的存在性和相关操作的相对时间顺序，为信息系统中的时间防抵赖提供基础服务。

3. 智能合约

“智能合约”这个术语是由尼克·萨博（Nick Szabo）在 1995 年首次提出的。他给出的定义是：智能合约是一套以数字形式定义的承诺。可以把智能合约理解为一种聪明的合约，它允许在没有第三方监督的情况下，进行可信性交易，这种交易可以追踪，且不能逆转。

可以把智能合约理解成 ATM 机、自动贩卖机或者咖啡机，他们都是在一定外界触发条件下或一定规则下，自动实现特定功能，并没有任何人为因素从中干预。在商业活动中，线上交易提出了简化交易的流程要求，同时还要提供对应的安全保证。而智能合约扮演的角色，就是将交易双方的条件和奖惩机制定好，让双方交易都在区块链上可以自动、忠实地去执行这份合约，让人工无从对其实施干预，这就是它的目的智能合约。

4. 共识机制

共识保证了区块链上的参与者可以互相信任，并且对下个区块进行验证。共识也确保了网络中的规则被遵守，同时承认在区块链环境下只有一个真理。

主流观点认为共识机制分为四大类：① 工作量证明机制（POW）；② 权益证明机制（POS）；③ 股份授权证明机制（DPoS）；④ 混合证明机制。

2.5.4 区块链的工作原理

(1) 区块。区块是一种记录交易的数据结构。每个区块由区块头和区块主体组成，区块主体只负责记录前一段时间内的所有交易信息，区块链的大部分

功能都由区块头实现，如图 2-8 所示。

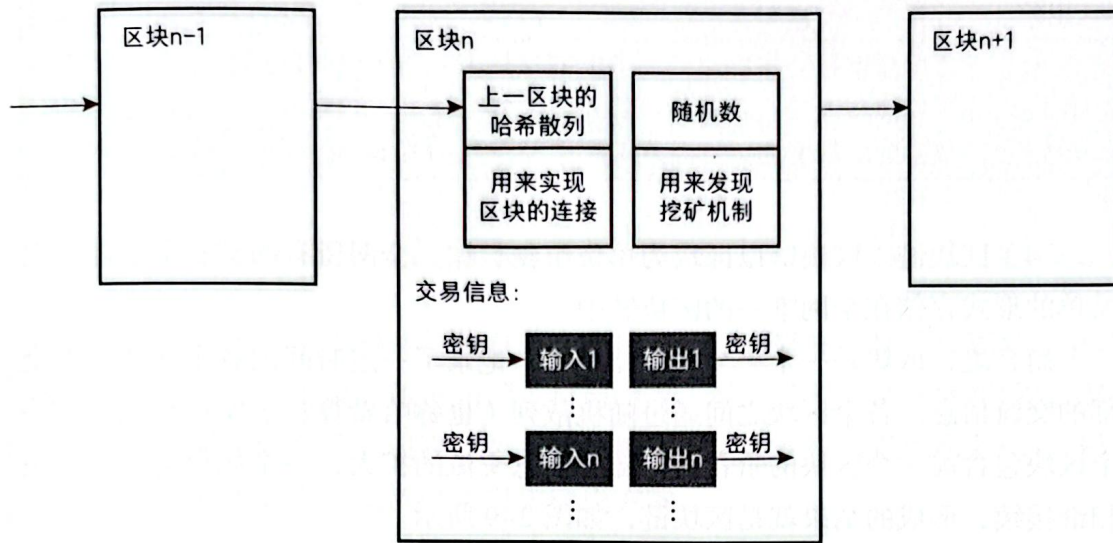


图 2-8 区块

(2) 区块头。区块头包括了以下信息。

- ① 版本号——标示软件及协议的相关版本信息。
- ② 父区块哈希值——引用的区块链中父区块头的哈希值，通过这个值每个区块首尾相连组成了区块链，并且这个值对区块链的安全性起到了至关重要的作用。
- ③ Merkle 根——这个值是由区块主体中所有交易的哈希值再逐级两两哈希计算出来的一个数值，主要用于检验一笔交易是否在这个区块中存在。
- ④ 时间戳——记录该区块产生的时间，精确到秒。
- ⑤ 难度值——该区块相关数学题的难度目标。
- ⑥ 随机数——记录解密该区块相关数学题的答案的值。

(3) 区块形成过程。区块的形成过程如表 2-7 所示。

表 2-7 区块的形成过程

步数	内容
第 1 步	在当前区块加入区块链后，所有矿工就立即开始下一个区块的生成工作
第 2 步	把在本地内存中的交易信息记录到区块主体中
第 3 步	在区块主体中生成此区块中所有交易信息的 Merkle 树，把 Merkle 树根的值保存在区块头中
第 4 步	把上一个刚刚生成的区块的区块头的的数据通过 SHA256 算法生成一个哈希值填入到当前区块的父哈希值中
第 5 步	把当前时间保存在时间戳字段中

续表

步数	内容
第 6 步	难度值字段会根据之前一段时间区块的平均生成时间进行调整以应对整个网络不断变化的整体计算总量，如果计算总量增长了，则系统会调高数学题的难度值，使得预期完成下一个区块的时间依然在一定时间内

(4) 区块链。区块链以区块为单位组织数据。全网所有的交易记录都以交易单的形式存储在全网唯一的区块链中。

简言之，区块是一个一个的存储单元，记录了一定时间内各个区块节点全部的交流信息。各个区块之间通过随机散列（也称哈希算法）实现链接，后一个区块包含前一个区块的哈希值，随着信息交流的扩大，一个区块与一个区块相继接续，形成的结果就是区块链，如图 2-9 所示。

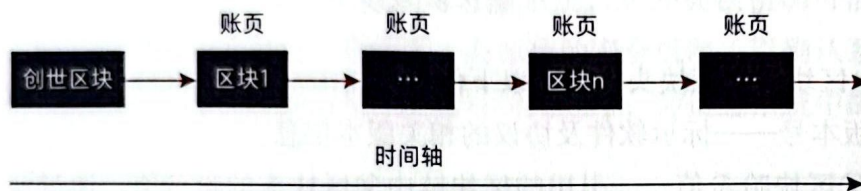


图 2-9 区块链

2.5.5 区块链的应用

区块链有三种应用模式，包括公有链、联盟链、私有链。优势各有不同，可供不同场景选择使用（见表 2-8）。其中，公有链是指任何人都可以随时参与到系统中读取数据、发起交易的区块链，典型代表应用为比特币；联盟链是指若干个机构共同参与管理的区块链；私有链则是所有参与结点严格控制在特定机构的区块链。

表 2-8 区块链的三种模式

类型	特征	优势	承载能力	适用业务
公有链	去中心化, 任何人都可以参与	匿名, 交易数据默认公开, 访问门槛低, 社区激励机制	10-20 笔 /s	面向互联网大众, 信任基础薄弱, 单位时间交易量不大
联盟链	多中心化, 联盟机构间参与	性能较高, 节点准入控制, 易落地	大于 1000 笔 /s	有限特定合作伙伴间信任提升, 可以支持较高的处理效率

续表

类型	特征	优势	承载能力	适用业务
私有链	中心化, 公司 / 机构内部使用	性能较高, 节点可信, 易落地	大于 1000 笔 /s	特定机构的内部数据管理与审计、内部多部门之间的数据共享, 改善可审计性



案例: 区块链
发票

与普通分布式技术相比, 公有链、联盟链、私有链在环境信任程度、篡改难度、业务处理效率方面各不相同。目前而言, 联盟链模式是金融领域应用的主要方向。对于中介成本过高、运行效率低下或无中介机构提供服务的业务场景, 都可以考虑运用区块链技术提供解决方案。

2.5.6 区块链的发展趋势

物联网、5G、人工智能和边缘计算等邻近技术将与区块链结合, 为网络参与者带来更高的价值。通过区块链技术, 使能未来网络中人、设备、服务的统一身份认证和管理, 使能人与机器、机器与机器之间的可信通信, 使能基于智能合约的多智能体实时交易, 这些将成为融合互联网、工业互联网乃至卫星通信网络的下一代未来网络的核心与关键。区块链确实有着变革互联网乃至人类社会的潜质, 要想真正发挥其潜能, 亦面临着不小的挑战, 比如自治、可信与监管问题。克服这些挑战, 有待区块链技术的进一步完善与创新, 也有待于目前监管体系的主动变革与创新。

监管专栏

金融科技技术基础相关监管政策

1. 大数据、人工智能相关法律法规

党中央、国务院高度重视大数据安全及其标准化工作, 将其作为国家发展战略予以推动。2015年9月, 国务院发布《促进大数据发展行动纲要》, 要求“完善法规制度和标准体系”“推进大数据产业标准体系建设”。2016年11月, 第十二届全国人民代表大会常务委员会通过了《中华人民共和国网络安全法》, 鼓励开发网络数据安全保护和利用技术。2016年12月, 国家互联网信息办公室发布《国家网络空间安全战略》, 在夯实网络安全基础的战略任务中, 提出实施国家大数据战略、建立大数据安全管理制度、支持大数据信息技术创新和应用要求。全国人大常委会和工信部、公安部等部门为加快构建大数据安全保