区块链技术及可信交易应用

张 勖 王东滨 邵苏杰 智 慧
北京同邦卓益科技有限公司研发团队 编著

北京邮电大学出版社
www.buptpress.com

区块链技术及可信交易应用

张　勖　王东滨　邵苏杰　智　慧　编著
北京同邦卓益科技有限公司研发团队

北京邮电大学出版社
www. buptpress. com

内 容 简 介

基于区块链的可信交易技术能够为融合新技术、新业态和新服务方式的现代服务业提供交易安全支撑，能够确保交易主客体信息真实、交易过程安全可信、交易可信透明、业务服务符合规范等。本书是作者在现代服务可信交易理论领域科研工作的总结，主要内容包括区块链发展和核心技术、现代服务业和可信交易，以及基于可信交易区块链平台的数据可信共享、信用评估、供应链应用，并以京东区块链为例介绍其在多行业中的应用。

本书可作为高等学校网络空间安全、计算机和电子信息类专业高年级本科生、研究生的学习参考用书，也可供相关领域的专业技术人员参考学习。

图书在版编目（CIP）数据

区块链技术及可信交易应用 / 张勖等编著. -- 北京：北京邮电大学出版社，2022.6

ISBN 978-7-5635-6661-7

Ⅰ. ①区… Ⅱ. ①张… Ⅲ. ①区块链技术 Ⅳ. ①TP311.135.9

中国版本图书馆 CIP 数据核字（2022）第 101165 号

策划编辑：马晓仟　　**责任编辑**：孙宏颖　　**封面设计**：七星博纳

出版发行：北京邮电大学出版社

社　　址：北京市海淀区西土城路 10 号

邮政编码：100876

发 行 部：电话：010-62282185　传真：010-62283578

E-mail：publish@bupt.edu.cn

经　　销：各地新华书店

印　　刷：唐山玺诚印务有限公司

开　　本：787 mm×1 092 mm　1/16

印　　张：10.75

字　　数：281 千字

版　　次：2022 年 6 月第 1 版

印　　次：2022 年 6 月第 1 次印刷

ISBN 978-7-5635-6661-7　　定价：39.00 元

前　言

现代服务业是融合新技术、新业态和新服务方式改造传统服务业，创造需求，引导消费，向社会提供高附加值、高层次、知识型的服务形态的行业。与此同时，现代服务业面临着参与交易主体间信任度低、交易过程不透明、结算可靠性不足、交易审计难等可信问题。而近年出现的区块链技术具有去中心化/分布式、去中介化、极难篡改、可追溯性、可编程性等特点，能够不需要中心化机构或者平台的信用评估与担保，实现在非信任环境下的多方间可信交易。基于区块链的可信交易技术和应用能够为构建可信社会交易体系和信任体系、促进现代服务业发展提供重要的技术保障和实现路径。

本书内容从现代服务业可信交易的关键技术和实践应用两个角度划分为上篇基础篇和下篇实践篇。本书共10章，包括上篇6章和下篇4章。第1章为区块链概述，包括区块链发展、区块链技术特点、区块链分类、区块链架构和典型区块链系统。第2章讲述区块链技术，包括区块链运行过程、区块链数据结构、区块链哈希运算、默克尔树、共识算法和智能合约。第3章阐述现代服务业和可信交易与区块链技术的关系，并侧重于介绍资产证券化和供应链金融领域区块链技术应用模式分析。第4章到第6章从现代服务业的典型应用，即数据共享、信用评估和供应链，阐述区块链技术应用于供应链、新能源互联网、企业与个人信用评估、供应链金融等场景的模式设计方案。第7章主要介绍区块链技术对产业和未来网络演进的意义和发展趋势。第8章至第10章以京东区块链为例介绍面向可信交易服务的区块链架构体系、典型应用、与智能技术融合发展等内容。

本书第1、2章由王东滨、智慧执笔；第3章由张勖执笔；第4、5、6章由邵苏杰执笔；第7、8、9、10章由姚乃胜带领的北京同邦卓益科技有限公司研发团队执笔。本书是在国家重点研发计划项目“现代服务可信交易理论与技术研究”（2018YFB1402700）的支持下完成的。来自北京邮电大学、北京同邦卓益科技有限公司、中国民航信息网络股份有限公司的作者在撰写本书的过程中，受到了北京航空航天大学、北京大学、北京科技大学、西安交通大学、清华大学、北京物资学院、赛迪工业和信息化研究院有限公司、中化能源股份有限公司、交通运输部科学研究院、北京德法智诚信息科技有限公司等项目组成员单位的各位专家、学者的指导，在此谨向以上各位表示衷心的感谢。

21世纪信息社会的颠覆性技术、创新应用不断涌现，现代服务业可信交易的相关理论和技术也处于持续发展和快速演进过程中。作者试图紧跟时代前进的脚步，但限于作者的学

识水平和表达能力，本书有限的篇幅很难反映区块链技术及其在可信交易应用中的全貌和发展趋势，书中难免存在疏漏和不当之处，恳请读者批评指正。此外，本书参考了大量专业论文、书籍和其他资料，如有引用遗漏或者给原作者带来任何不便，恳请与我们联系，我们将及时响应并更正。

目　录

上篇　基础篇

下篇　实践篇

上篇

基础篇

第1章 区块链概述

区块链是一种块链式存储、不可篡改、安全可信的去中心化分布式账本，结合了分布式存储、点对点传输、共识机制、密码学等技术。近年来，区块链因应用于比特币等加密货币而获得了极大的关注，区块链技术的研究与应用呈现快速增长的趋势。在不久的将来，区块链技术极有可能会改变我们的交互、生活，甚至触发下一次产业革命的颠覆[1]。在本章中会对区块链的发展、区块链的技术特点以及其分类等进行展开介绍。

1.1 区块链的发展

区块链的发展总体可分为三个阶段：区块链1.0主要应用于数字货币；区块链2.0实现了可编程金融，增加了智能合约的支持；区块链3.0旨在落地各行各业基于区块链的应用，构建可信、智能的社会生态。

1. 区块链1.0

区块链技术和理论最初来源于比特币，2008年中本聪首次提出了区块链这种数据结构，以及基于区块链的比特币[1-2]。比特币的交易数据是写在区块中的，各区块都带有时间戳，区块和区块之间通过哈希指针串联起来并形成时序关系，一旦篡改某一个区块中的数据，其之后所有区块中的哈希值都需要更改，这种记账方式使得比特币极难篡改。并且比特币作为一种分布式记账技术，整个交易过程无须第三方机构组织验证或监督，而是由区块链系统中的各个节点来验证交易的合理性。在区块链网络中，各节点时刻监听网络中广播的数据，当接收到其他节点发来的新交易和新区块时，它首先验证这些交易和区块是否有效，包括数据中的数字签名、区块中的工作量证明等，只有验证通过的区块才会被处理和转发[3]。

区块的产生过程也叫挖矿，比特币通过出块奖励和手续费来激励矿工记账和打包数据成块，比特币规定每产生21万个区块，出块奖励的比特币将减半。2009年年初，比特币系统正式上线，中本聪挖出了第一个区块，即“创世区块”，产生了最初的50个比特币。比特币在2020年5月完成了第三次产量减半，出块奖励已经减半为6.25个BTC(Bitcoin)。据CoinGecko的数据显示[4]，截至2022年2月，当前加密货币市值为1.97万亿美元，其中比特币市值就占了40.6%。自2013年10月以来比特币价格走势如图1-1所示[5]。

继比特币之后，市场中涌现了很多种类的加密货币，据Statista的统计，如图1-2所示，截至2022年2月，存活的加密货币有10 397种[6]。2011年莱特币(LTC)面世，莱特币在技术原理上与比特币基本相似，它使用硬内存和基于Scrypt(一种加密算法)的挖矿工作量证明算法，

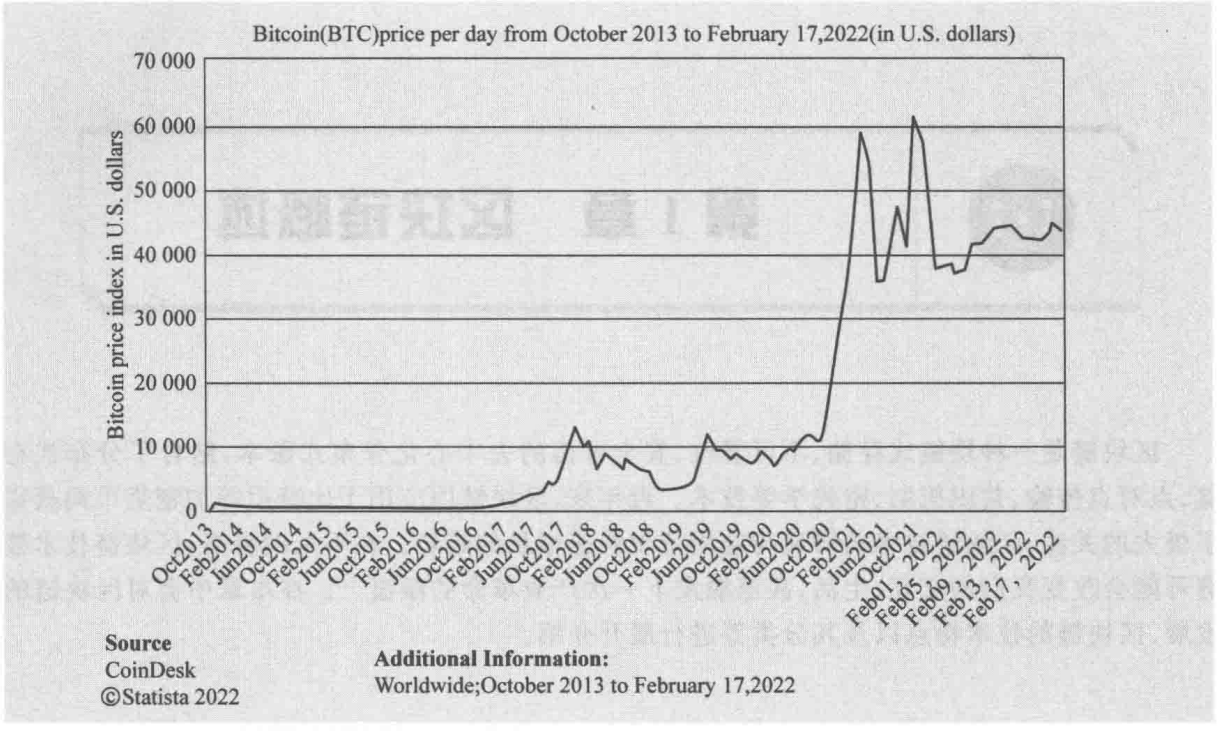

图 1-1　比特币历史价格图(2013 年 10 月至 2022 年 2 月)

使得在普通计算机上挖掘莱特币更加容易,降低了挖矿硬件成本。2013 年瑞波(Ripple)网络[7]被推出,随之发行了瑞波的基础货币瑞波币。瑞波网络是世界上第一个开放的支付网络,通过瑞波网络可以转账任意一种货币以及快速完成交易确认。2016 年 10 月 28 日,零币(Zcash)项目发布,Zcash 是首个使用零知识证明的区块链系统,零知识证明指的是证明者不需要向验证者提供任何有用信息,就可以使得验证者得出某论断是正确的,所以 Zcash 系统可以实现匿名支付。

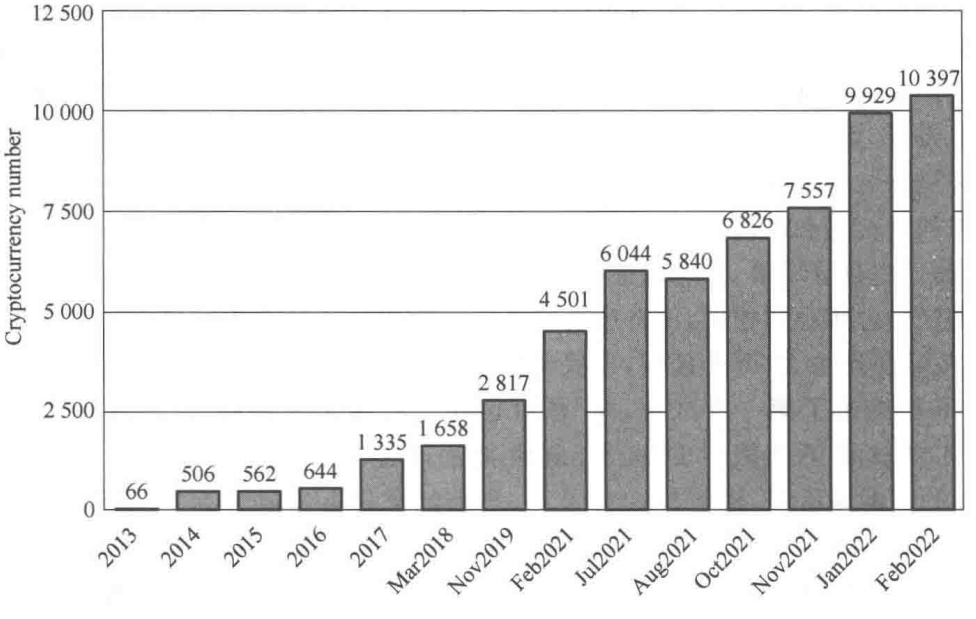

图 1-2　加密货币数量历史数据图(2013 年至 2022 年 2 月)

2. 区块链 2.0

为了解决比特币的难以扩展，无法自定义信息结构（如资产、身份、股权）等问题，以太坊应运而生。2013 年 11 月 Vitalik Buterin[8] 发起了以太坊项目，并在 12 月发布了《以太坊白皮书》。2014 年 4 月，以太坊联合创始人 Gavin Wood 发表了《以太坊黄皮书》，并将其作为以太坊虚拟机的技术说明。以太坊是一个开源的有智能合约功能的公共区块链平台，允许用户在上面搭建各种去中心化的应用。在无可信第三方验证的情况下，智能合约作为一种监控、验证、执行合约条款的计算机交易协议，嵌入由数字形式控制的价值实体，担任合约双方共同信任的代理，自治、高效、安全地执行合约。以太坊的核心是图灵完备的以太坊虚拟机。用户可以使用高级编程语言或者专门用于智能合约开发的语言 Solidity 编写智能合约，并可将智能合约部署在以太坊区块链上，然后在以太坊虚拟机中运行。以太坊智能合约的执行需要消耗燃料（gas）费，用以维护以太坊网络，燃料费不足智能合约就会停止执行。以太坊适用于公有链、私有链和联盟链 3 种区块链环境，不同的区块链环境可以通过扩展包的形式将智能合约部署到链上。

2015 年 12 月，Linux 基金会发起了超级账本 Hyperledger 开源区块链项目[9]，旨在构建业务驱动的、跨行业的商业区块链平台，其中 Fabric 项目最受关注，其专门针对企业级区块链应用。Hyperledger 中的智能合约称为链码，通过调用链码中的函数方法来实现处理交易的业务逻辑，完成对分布式账本的更新和维护。2016 年 4 月，R3 公司发布了面向金融机构定制设计的分布式账本平台 Corda，其保障了数据仅对交易双方及监管可见的交易隐私性。R3 公司发起的联盟包括花旗银行、汇丰银行、德意志银行、法国兴业银行等 80 多家金融机构[2]。

3. 区块链 3.0

随着区块链 2.0 智能合约的引入，区块链技术开始不仅在金融领域得到发展，在物流、医疗、司法、公证、投票等其他领域也投入运用，2020 年全球区块链企业垂直分类[10] 如图 1-3 所示。一方面区块链针对已有业务，其应用场景正在实体经济、公共服务等传统领域不断拓展，呈现新型水平化布局；另一方面随着应用场景的深入和多元化，区块链要发挥更多的“互联网信任基座的变革潜力”[11]。

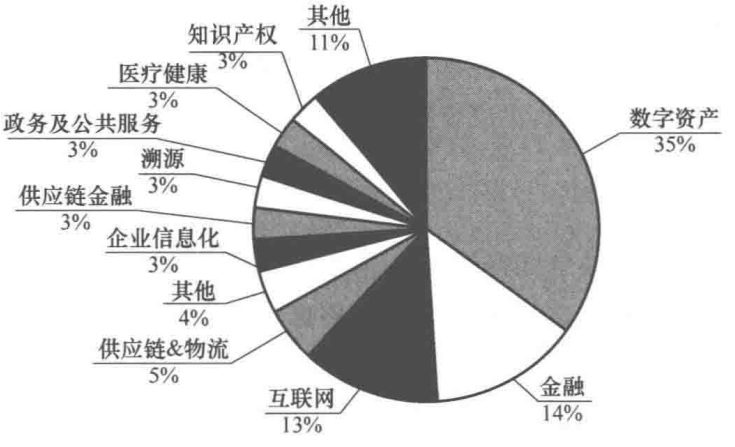

图 1-3　2020 年全球区块链企业垂直分类

在应用落地方面，区块链技术已经对一些行业进行了革命性的改变。例如：

① 医疗。区块链技术有可能彻底改变患者记录和个人信息的管理和存储。此外，区块链可以优化不同医疗服务之间的通信，从而促进全球协作。

② 运输。物流供应链在运输和交付服务中，可以通过引入分布式账本技术进行深度优化。区块链记录可用于优化货物的可追溯性和问责制。

③ 投票。随着透明的公共分类账被集成到投票系统中，该过程变得更易于访问且更安全。

在新兴应用方面，区块链技术不可篡改、可追溯、无中介化和分布式的特点使其可以赋能数字人民币，进行碳追踪、碳交易等。区块链还可以为物联网数据流转和价值挖掘提供可信保障，其特性可以让隐私数据变得有据可寻，提供安全性和透明度。由于云资源的开放性和易得性，所以公有云平台成为当前区块链创新的最佳载体，蚂蚁、腾讯、华为等主流云厂商的 BaaS 平台(Blockchain as a Service，区块链服务)已经具有多引擎支持、多模式部署、多节点统一管理的能力。区块链也被寄予厚望，或许可以颠覆现有中心化的互联网，成为 Web 3.0 的天然基石，实现无服务器的、去中心化的、可验证的和安全的互联网。

1.2 区块链的技术特点

区块链作为一种全新的去中心化/分布式基础架构与分布式计算范式，其主要技术特点如下。

(1) 数据不可篡改

不可篡改性指的是一旦数据经过验证被写入区块链后，任何人都无法对数据进行修改和抵赖。区块链利用哈希函数的强抗碰撞行和单向性以及数字签名的防伪认证，保证了其不可篡改性。

(2) 去中心化/分布式

在网络层面，区块链网络节点间的传输采用 P2P 协议，即任何节点都是平等的且不存在中心节点。在控制层面，不存在中心控制节点，交易数据和区块数据区块链数据的写入和同步需要多数节点验证数据达成共识，再决定哪些数据可以写入。根据去中心化的程度，不同区块链系统应用不同的共识机制。

(3) 可追溯性

区块链采用带时间戳的块链式存储结构，有利于追溯交易从源头状态到最近状态的整个过程。时间戳作为区块数据存在的证明，有助于将区块链应用于公证、知识产权注册等时间敏感领域。

(4) 智能合约

由传统的外置合约发展为内置合约，基于区块链的双方之间不仅可以进行简单的价值转移，用户还可以通过编写智能合约把预设的规则和条款转化为可以自动执行的程序，将智能合约部署在区块链上，一旦满足条件智能合约就会自动执行，部署后智能合约的逻辑将再也无法更改。

1.3　区块链的分类

根据节点准入机制，区块链系统可以分为许可链和非许可链。许可链的节点需要中心机构的审查，因此这些节点是可信的；也可能这些节点仍然互不信任，需要协商维护规则和访问控制，只有经过授权的节点才能访问数据以及参与系统维护。非许可链不对节点进行身份审查，节点皆以匿名形式自由地加入或退出网络[4]。根据去中心化程度，区块链系统可以分为公有链、联盟链和私有链 3 类，非许可链对应的是公有链，许可链可以按照私有程度的不同分为联盟链和私有链，这 3 类区块链的对比如表 1-1 所示。

表 1-1　3 类区块链的对比

特　征	公有链	联盟链	私有链
参与者	任何人自由进出	企业或联盟成员	个体或公司内部
共识机制	PoW/PoS/DPoS 等	分布式一致性算法	分布式一致性算法
激励机制	需要	可选	不需要
中心化程度	去中心化	多中心化	(多)中心化
数据一致性	概率(弱)一致性	确定(强)一致性	确定(强)一致性
网络规模	大	较大	小
处理交易能力	$3\sim20/s^{-1}$	$1\,000\sim10\,000/s^{-1}$	$1\,000\sim200\,000/s^{-1}$
典型应用	加密货币、存证	支付、清算	审计

由于公有链系统对节点是开放的，公有链通常规模较大，所以达成共识难度较高，吞吐量较低，效率较低。在公有链环境中，由于节点数量不确定，节点的身份也未知，因此为了保证系统的可靠可信，需要确定合适的共识算法来保证数据的一致性和设计激励机制去维护系统的持续运行。典型的公有链系统有比特币、以太坊。

联盟链通常是由具有相同行业背景的多家不同机构组成的，其应用场景为多个银行之间的支付结算、多种企业之间的供应链管理、政府部门之间的信息共享等。联盟链中的共识节点来自联盟内各个机构，且提供节点审查、验证管理机制，节点数目远小于公有链，因此吞吐量较高，可以实现毫秒级确认；链上数据仅在联盟机构内部共享，拥有更好的安全隐私保护。联盟链有前文介绍过的 Hyperledger、Fabric、Corda 平台和企业以太坊联盟等。

私有链通常部署于单个机构，适用于内部数据管理与审计，共识节点均来自机构内部。私有链一般网络规模更小，因此比联盟链效率更高，甚至可以与中心化数据库的性能相当。联盟链和私有链由于准入门槛的限制，可以有效地减小恶意节点作乱的风险，容易达成数据的强一致性。

1.4　区块链的架构

2016 年袁勇等[5]提出了区块链基础架构的“六层模型”，如图 1-4 所示，从底层到上层依次是数据层、网络层、共识层、激励层、合约层和应用层。数据层包括区块结构和数据加密等技

术；网络层包括网络结构、数据传播技术和验证机制等；共识层包括 PoW（工作量证明）、PoS（权益证明）、DPoS（授权股份证明）等多个网络节点之间的共识机制；激励层包括激励的发行和分配机制；合约层包括各种脚本代码和智能合约；应用层包括数字货币等应用场景。

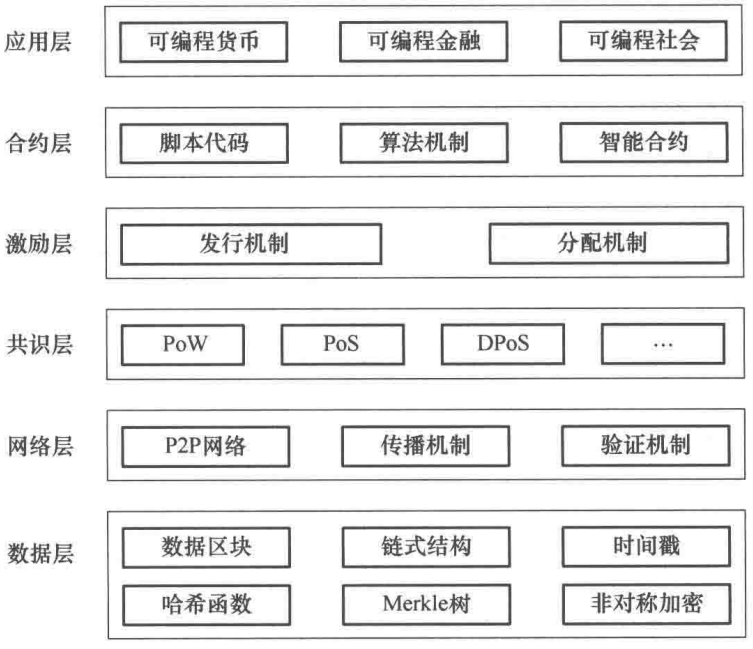

图 1-4　区块链基础架构的“六层模型”

1.4.1　数据层

数据层负责区块链数据结构和物理存储，区块链的数据结构表示为交易被排序的区块链表，如图 1-5 所示。区块记录一段时间内的交易记录，将一段时间内收到的交易记录封装到一个数据区块中，在区块的头部包含块的元数据，元数据主要包括区块当前版本、父区块的哈希值、Merkle 树根哈希（用于有效总结区块中所有交易的数据结构）、区块创建时间、区块当前难度和一个随机值，区块头用于验证区块的有效性。每个区块头都连接着前一个区块，这使得区

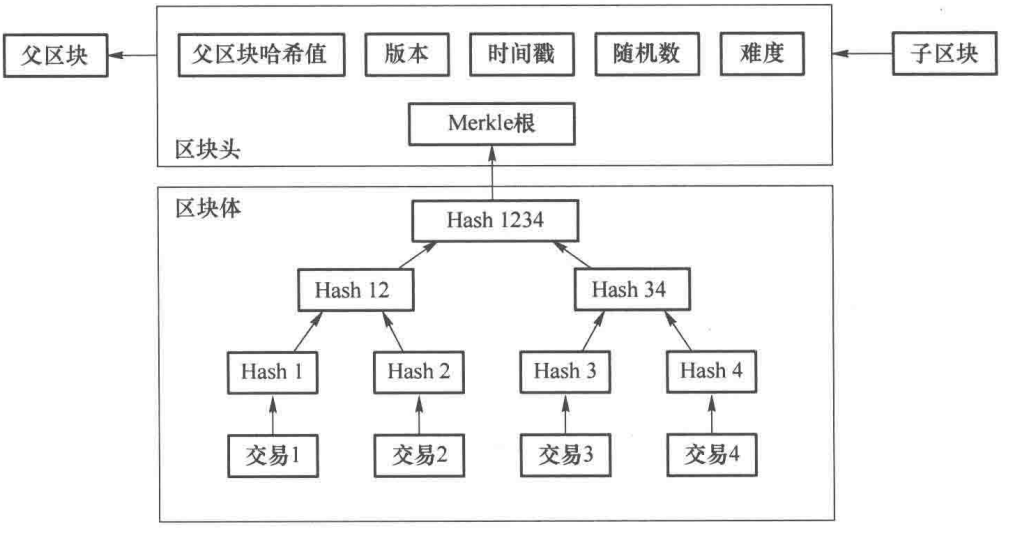

图 1-5　区块结构